
NO. 20
November 2011 • Price Free • www.networkset.net
NetWork Set
First Arabic Magazine For Networks
شبكات المستقبل VLC
Visible Light Communication
Antenna
Polarization
رحلة في أعماق روتر
الهجوم على
الشبكات اللاسلكية
من هم الهاكرز ؟
طرق الانتقال من
IPv4 إلى IPv5
TCP-Intercept
ما هو الـ DNS ؟؟؟
Domain Name System
رسالة شكر وتقدير مقدمة لكل المشاركين معنا في المسابقة الخاصة بالمحتوى العربي
لمساهمتهم ومشاركتهم في المسابقة وكونهم أكثر إيجابية من غيرهم

التدوين في سطور

عام كامل وأنا أعد الأصدقاء والمتابعين بأنّي سوف أتحدث عن التدوين وفوائده, ودائماً ما كنت أُؤجّله لموعد آخر حتى أصل إلى غايةٍ كنت قد خطّطت لها من البداية, لكنّي تأخرت لظروف خارجة عن إرادتي , لكن بعد المسابقة التي أقمتها على المدونة, وعدد المشاركات الضئيل نسبياً قررت أن أكتب عن فوائد التدوين حتى يندم بعض المهندسين على عدم مشاركتهم هذا العالم الكبير .

قد تتصور أنّ التدوين والكتابة هو شيء سوف يجعلك تُقدم ما لديك من المعلومات لعامة الناس كمساهمة منك في المساعدة فقط , نعم هذا صحيح, لكن مهما علمت وملكت من معلومات سوف تصل يوماً ما إلى نقطة تجد نفسك فيها قد كتبت كل ما تعلمه, هذا الشعور صادفته بعد شهر واحد من إطلاقي للمدونة , هل تصدق ؟!!. هذا الشيء جعلني أبدأ البحث والقراءة في المدونات والمواقع الإنكليزية للحصول على أفكار مناسبة للكتابة عنها, والحمد للّه حصلت على الكثير من الأفكار, لكن كلها كانت تنتهي بسرعة كبيرة كون التدوين مسبقاً كان بمعدل خمس تدوينات إسبوعياً , وفي كل مرة تنتهي الأفكار كنت أبدأ البحث من جديد عن أفكار جميلة يمكن الكتابة عنها, وكانت الخيارات في البداية تصبح صعبة مع الشروط التي وضعتها بخصوص أهمية الموضوع وتخصّصه وعدم تكراره على ساحة المحتوى العربي .

مع مرور الوقت أصبحت أهمية موضوع التدوين بالنسبة لي مثل أهمية الأوكسجين الذي أستنشقه, فهو الشيء الوحيد الذي سوف يضمن لك أن تبقى متصل بشكل دائم مع عالم الشبكات وخصوصاً أنّه أياً منّا قد يصل أحياناً إلى أوقات يجد فيها نفسه لا يريد أن يقرأ أو أن يتعلم شيء جديد , وأحياناً يصل إلى مرحلة الملل من الشبكات ومن عالمه ومن بروتوكولاته , ولكن ارتباطي بالتدوين وشعوري بأنّ هناك الكثير من ينتظر الجديد من المدونة جعلني لا أتوقف يوم واحد عن التدوين, وبالتالي قراءة وتفكير المواضيع والمقالات التي يجب أن أكتب عنها وهي أهم فوائد أن تكون مُدوِّن – الارتباط الدائم بالمجال الذي تعمل أو تدرس فيه - فعملية اختيار الموضوع تجبرني أحياناً أن أبقى يومان أو ثلاثة منغمساً في صفحات الإنترنت والمدونات والمواقع العالمية لاختيار أفضل موضوع يمكن الكتابة عنه , وبالتالي كنز حقيقي تحصل عليه أثناء بحثك عن أفضل مقال.

الفائدة الثانية هي المعلومة نفسها , عندما تقرر الكتابة في موضوع معيّن يجب أن تملك ثلاث أشياء : الفهم الكامل للموضوع , القدرة على التبسيط , القدرة على الرد عن أي سؤال مطروح , لو نظرت إلى هذه الأمور الثلاث لأدركت أنّ اختيارك لأي موضوع يحتاج منك أن تقرأ وتفهم الموضوع نفسه بشكل كبير جداً وخصوصاً مسألة التبسيط, لأنّ القاعدة الأولى في التدوين هي : تبسيط المعلومة وتيسير فهمها, لأنّ هذا الأمر يدل على فهمك الكامل للمعلومة وتعقيدها يعني عدم استيعابك أنت نفسك لما تكتب فأحذر من هذه النقطة , عندما أختار الموضوع المناسب وهو أصعب ما في التدوين أبدأ عملية جمع المعلومات والتي أحياناً تدفعني إلى قراءة خمسين مقال إنكليزي عن الموضوع نفسه أو قراءة الفقرة كاملة من عدة كتب ومراجع إنكليزية وبالتالي تخيل معي المقدار الكبير من المعلومات التي تقرأها وتتعلمها بخصوص موضوع معيّن !!!.

بعد الفترة الطويلة التي قضيتها في التدوين والتي تكللت بحوالي 300 مقال احترافي تخصّصي, وصلت إلى مرحلة متقدمة والحمد للّه وهي إمكانية الكتابة عن أي موضوع يخص مادة الشبكات, بالإضافة إلى إمكانية جعل أي موضوع مهم بنظر القارئ, وتوصلت أيضاً إلى إمكانية إيجاد عشرات الأفكار المميزة والتي يمكن الكتابة عنها في فترة قصيرة جداً وهناك ميّزة مهمة جداً لن أبوح بها الآن وسوف أتركها ليوم مقرر عند اللّه !.

لو تجاهلنا كل هذه الفوائد الشخصية, ونظرنا إلى الأمر بنظرة سماوية ربانية, فسوف تجد الأمر شيء لا يمكن وصفه بالكلمات, وبالأخص عندما تجد تعليق أو رسالة طويلة تصلك من أحد الأشخاص وهو يشكرك ويثني عليك ويدعو لك من قلبه, فهي المتعة واللذة التي أصبحت أهم ما أنتظره من التدوين , بالإضافة إلى ذلك ستجد نفسك مرتاح نسبياً ونفسياً مع اللّه لأنّك تقوم بأداء جزء بسيط من واجبك نحو إخوانك وأصدقائك وطالبي العلم في عالمنا العربي, وخصوصا أن الدنيا أصبحت في الآونة الآخيرة دنيا تحكمها المادة والفساد, وأصبح كل واحد يعبد المال والوظيفة , وأخيراً هل اقتنعت بالتدوين أم مازلت متأثراً بالدنيا المادية ؟ ودمتم بود .

أيمن النعيمي - سوريا





مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

www.networkset.net



NetWork Set

First Arabic Magazine For Networks



شبكات المستقبل VLC

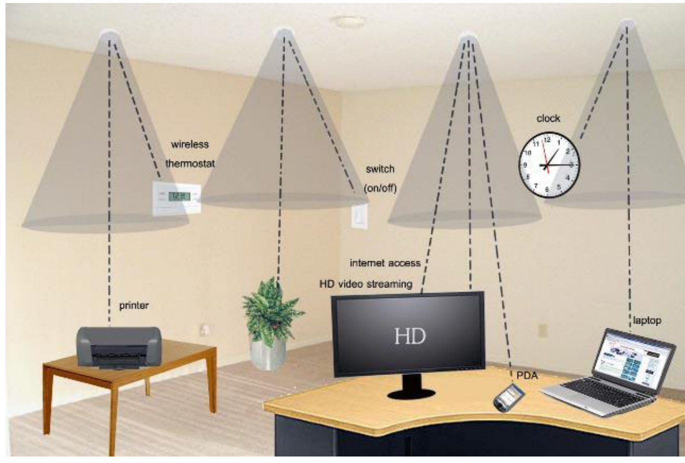
Visible Light Communication

معظم الأشياء قد تتعدد استخداماتها إلى جانب الغاية الأساسية من تصنيعها، فمثلاً الهاتف الجوال صنع أساساً لغرض الاتصال وأيضاً لتشغيل الملتيميديا والتطبيقات كاستعمال ثانوي , وكذلك الكمبيوتر له عدة استخدامات وغيرها من الأجهزة. ولكن ما هي الاستعمالات الثانوية لأجهزة الإضاءة ؟ وهل فكرت يوماً أن تقوم بتحميل هذه المجلة عن طريق الإنارة التي في الغرفة ؟

الباحثون والعلماء وكالعادة يحاولون استنزاف الأشياء واستخلاص كل طاقتها الممكنة، لذلك فكّروا في الاستفادة من الإضاءة وكيفية استغلالها أشد استغلالٍ والنتيجة كانت تقنية تجري عليها الأبحاث حالياً لتطويرها من قبل العلماء , وبالأخص في معهد فراونهوفر هاينريش هيرتز وبالتعاون مع مختبرات خاصة بشركات عالمية رائدة في مجال الإلكترونيات مثل شركة سيمينز و فرانس تيليكوم أورانج. هذه التكنولوجيا ستغير مفهوم العالم للاتصال , وتُعرف بمصطلح الـ VLC.

الـ VLC (Visible Light Communication) أو الاتصال عبر الضوء المرئي , وتعريفها ببساطة هي تقنية تسمح للأشخاص بالاستفادة من أجهزة الإنارة -إلى جانب إضاءتها- لنقل البيانات عبرها والدخول إلى الانترنت باستعمال الضوء العادي القادم من تلك الأجهزة فقط.

يقول البروفسور ناكاغاوا الذي يرأس الكونسرسيوم الصناعي الياباني للاتصالات عن الضوء المرئي «إن الضوء مستخدم يومياً بالفعل منذ زمن طويل من قِبَل ملايين الأشخاص لنقل المعلومات , وعلى سبيل المثال عندما يستخدم مشاهد تلفزيوني جهاز التحكم عن بعد الذي يعمل بالأشعة تحت الحمراء لتغيير القنوات إلّا أنّ هذه الوسيلة لنقل البيانات باستخدام ضوء الأشعة تحت الحمراء يقع خارج مجال رؤية العين البشرية».



الفكرة واضحة ولا تحتوي أي تعقيد وهي نقل البيانات باستخدام موجات الضوء الذي تردده يتراوح بين 400 و800 تيراهيرتز. ولتوليد ضوء بهذا التردد نستطيع استخدام مصابيح الفلوريسنت العادية حيث وصلت سرعة نقل البيانات بواسطتها إلى 10 كيلوبت في الثانية أو باستخدام مصابيح الـ LED بسرعة نقل وصلت إلى 500 ميكابت في الثانية ولمسافة قليلة جداً لا تتعدى الـ 5 أمتار فقط ! لكن في مايو الماضي، تمكن الباحثون من إضاءة غرفة مساحتها أكثر من 10 متر مربع، وفي الوقت نفسه من نقل بيانات ولكن بسرعة لم تتعدى الـ 100 ميكابت في الثانية من دون أية مشكلة أو عرقلة في عملية الإرسال أو الاستقبال. وهذا يعني أنّه من الممكن تشغيل أربعة أفلام فيديو بوضوح على أربعة كمبيوترات في الوقت ذاته، وذلك طبقاً لما قاله أحد الباحثين بالمعهد. أيضا بدأت هذه التقنية



بمجاراة الايثرنت ، حيث أمكن إرسال بيانات بسرعة 10 ميكابت في الثانية ولمسافة 1 إلى 2 كيلومتر وذلك باستعمال مصابيح LED بطاقة عالية وذات إضاءة نافذة. ومؤخراً حدثت النقلة النوعية عندما نجح باحثو المعهد المذكور في نقل بيانات بسرعة تصل إلى 800 ميكابت في الثانية بواسطة أضواء مصابيح LED ذات ألوان مختلفة من أحمر وأزرق وأخضر وأبيض داخل المختبر.

استعمال الـ LED وتفضيلها جاء بسبب أنّ هذه المصابيح تعتبر ذات إضاءة عالية تنتشر إلى مسافات بعيدة , لذلك فهي تستخدم في حالة الضباب والإنذار في سيارات الشرطة والإسعاف لكونها صغيرة الحجم ومتنوعة الأشكال إضافة إلى أنّها موفِّرة للطاقة وطويلة العمر وصديقة للبيئة. ومؤخراً نجح مهندس في شركة كاسيو في أن يلتقط بكاميرا خاصة من الأرض إشارة منبعثة من مصباح وضع على قمة برج طوكيو التي تبعد 250 مترا عن مكانه.



كيف تعمل هذه التقنية ؟

تقوم هذه التقنية على أساس تضمين (Modulation) الإشارة المرسلة مع انبعاث الضوء , أي أنّها تضمن موجات داخل موجات , وفكرتها هي أنّ هذه الإضاءة تغلق وتفتح بتردد عالي يقدّر بآلاف المرات , وبسرعة عالية جداً والتي لا تستطيع العين البشرية ملاحظتها وتمييزها وتعتبرها مضيئة دائماً، حيث يكون عملية إرسال المعلومة عن طريق هذا الإغلاق والفتح لتمثيل الصفر والواحد في لغة الكمبيوتر وهو نوع من الـ Modulation يسمى OOK On/Off Keying. قد يسأل البعض وكيف نستقبل الإشارة إذا أطفأنا الإنارة؟

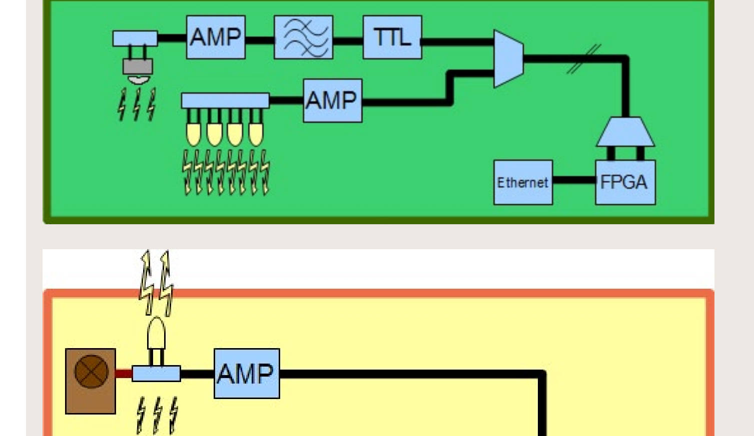
الجواب هو : إنّ هذه التقنية تعمل حتى ولو كانت الإنارة مطفئة وستقوم بالتوصيل، حيث أنّ الإنارة هنا سيتم تحويرها لكي تبقى هناك ومضات غير محسوسة هي التي تقوم بعملية النقل. حيث أنّ تغذيتها بتيار ضعيف يمكن أن تسمح لها بإصدار الفوتونات التي تقوم بالنقل. أمّا الخيار البديل فيمكن أن يكون تصميم دايودات باعثة للضوء تتضمن مصادر ضوئية تبث بترددات غير مرئية لتحقيق هذه الوظيفة حين إطفاء أنوار الغرفة.

أمّا طريقة استقبالها فهي تحتاج إلى جهاز مستقبل خاص يكون أشبه بالمودم يقوم باستقبال هذه الومضات ونقلها إلى دائرة إلكترونية لتحويلها إلى إشارات مفهومة. من أهم مكوناته ببساطة هو متحسس ضوئي Photodetector , وهو عبارة عن قطعة إلكترونية تقوم بتحويل الضوء الساقط إلى فولتية أو تيار. وهي على عدة أنواع , مثل : الدايود الضوئية Photodiodes، الترانسستر الضوئي Phototransistors، أو المقاومة الضوئية Photoresistors.

ومن أهم الأشياء إنّه يمكن استعمال الـ LED نفسه للإرسال والاستقبال , حيث يمكنه استقبال أطوال موجية محددة وبحساسية قليلة لبعض الألوان وحسب الطول الموجي لكل منها , ولكن يعتبر هذا مقبولاً مقارنة مع المكونات المصنوعة خصيصاً كمستقبلات للضوء.

فمثلاً يمكن للـ LED الأخضر التحسس بالضوء الأزرق والأخضر ولا يمكنه التحسس للأصفر والأحمر، وهذا يعتمد على لون الـ LED ليمكن استعماله كمرسل ومستقبل وبأزمان مختلفة.

وهنا مثال لدائرة إلكترونية تمثل الـ Access point والصورة التالية تمثل جهاز End user.



كما يمكن لكاميرا الهاتف النقال أو الكاميرا الديجيتال التقاط وتحسس هذه الإشارات , حيث تتكون هذه الكاميرات من مصفوفة من المتحسسات الضوئية على عدد البكسلات وكل منها يستطيع استقبال الضوء المسلط عليها وذلك بدعم تطبيق برمجي يتم تثبيته لترجمة هذه الإشارات وهو بمثابة تحوير لعمل الكاميرا. وبفضل وجود أكثر من متحسس بدلاً من واحد نستطيع استقبال الإشارة على عدة قنوات اتصال , حيث تُمثّل كل قناة بمتحسس والذي بدوره يمثل بالبكسلات الخاصة بالكاميرا.

ومن الحلول لنظام الإرسال والاستقبال في هذه التقنية بشكل عام في الاتصال الـ Full Duplex، اقترح الباحثون أن يكون إحدى هذه الطرق :

- ممكن أن يكون الاستقبال بطول موجي معيّن مثل الضوء العادي والإرسال بطول موجي آخر مثل أشعة الـ IrDA.
- أيضاً ممكن عزل الإرسال والاستقبال عن طريق الوقت , أي أنّ الإرسال يكون بفترة زمنية معيّنة وبعدها يكون الاستلام بفترة زمنية معيّنة أيضاً, كما يمكن نقل الإشارات بتقنية TDM المستخدمة في الاتصالات عن طريق تقسيم الزمن .
- من الاقتراحات الأخرى هو استخدام موجات الراديو في الإرسال وخاصة في الانترنت , حيث يكون بكميات قليلة وبذلك استطعنا الاستفادة من مميزات كل تقنية .
- وأخيراً هناك بعض الأجهزة مصممة للخدمات أو التطبيقات التي لا تحتاج إلى إرسال بيانات كما في الراديو والتلفزيون , لهذا فلا داعي لوجود دائرة إرسال أصلاً.

كيف يمكننا الاستفادة منها ؟

يمكننا استغلال هذه التقنية وتطبيقها في عدة مجالات و أهمها هو الدخول إلى الانترنت والتي تعتبر الغرض الأساسي و كذلك التنقل بين أجهزة الشبكة، لذلك تتنوع استعمالاتها بين الشبكات وبين مجال الاتصال بشكل عام ومن هذه الاستخدامات :

- تعتبر حل مناسب في الأماكن التي تزدحم فيها إشارات أجهزة الواي فاي والأجهزة التي تستعمل الموجات الراديوية , حيث تكون أكثر عرضة للضوضاء والتداخل فيما بينها , فعلى سبيل المثال : تزويد الانترنت في الطائرات وذلك لتجنب التشويش على أجهزة الاتصال فيها، فقريباً جداً سيكون بمقدور الركاب استخدام شبكة الإنترنت على أجهزتهم الخاصة أثناء السفر، في الوقت نفسه سيوفر لمصنعي الطائرات مبالغ طائلة يتم إنفاقها في إنشاء كيلومترات من الكابلات .
- تستعمل في الأماكن الخاصة والسرية والتي تحتاج إلى تأمين الدخول إلى الشبكة كون البث لا يتعدى الجدران إلى باقي أجزاء المبنى كما في باقي التقنيات وينحصر في الغرفة التي تحتوي الأجهزة فقط
- يمكن أن تكون البديل الأمثل للشبكات التي تستعمل الموجات الراديوية المضرة وخصوصاً التي تبث بقدرات عالية , حيث تعتبر الـ VLC غير مضرة للصحة ولا تشكل أي خطورة .
- كذلك يستعمل في الأماكن التي يكون فيها البث بالموجات الراديوية ممنوعاً ويحتاج إلى ترخيص كما في المواقع العسكرية .
- أيضاً يمكن استعمالها لإيصال الربط بين أجهزة الـ GPS داخل البنايات والأقمار الصناعية وحيث إن اتصال الـ GPS يتطلب وجود فضاء مفتوح للاتصال بالأقمار الصناعية، وبذلك ساهمت في حل بسيط لهذه المشكلة.
- يمكن استخدامها داخل المصانع، ففي كثيرٍ من الأحيان تؤثر الشبكات الراديوية اللاّسلكية سلباً على كفاءة وفاعلية الأجهزة وبالتالي على عجلة الإنتاج
- يمكن استخدامها في المستشفيات على سبيل المثال، حيث يمكن توظيف جزء من قدرة مصابيح غرفة العمليات في توجيه روبوت داخل غرفة العمليات أو تشغيل أجهزة الغرفة أو جهاز أشعة الإكس راي .
- من ناحية الاتصال يمكن الربط عن طريقها بين جهاز وآخر، حيث يمكننا عمل شبكة بين هاتفين أو لربطها مع الكمبيوتر، إضافة إلى ذلك في شهر يوليو من هذا العام 2011 وبالتحديد في مؤتمر TED العالمي تم أيضاً تقديم أول تجربة نقل فيديو بنقاوة HD وعرضه على التلفزيون باستخدام تقنية الـ VLC , ويمكن تطبيق غيرها من الأمثلة على ذلك .

- يمكن استعمالها للاتصال بين الغواصين بسبب صعوبة إمكانية الاتصال بواسطة الإشارات الراديوية تحت الماء , وأيضاً لإعطاء بعض المعلومات عن البضائع في الأسواق , وكذلك في تبادل المعلومات بين الإشارات المرورية ولوحات الإرشاد و التحذيرات بشأن الاختناقات المرورية أو الحوادث بين السيارات في الشوارع .

ماذا يميزها عن غيرها من التقنيات ؟

- أكثر أمان من الشبكات اللّاسلكية الأخرى .
- يمكن زيادة مدى الاتصال بزيادة قوة الإضاءة من دون خطورة على العينين وهذا الأمر مستحيل مع الأشعة تحت الحمراء .
- تكلفتها المنخفضة .
- سهولة انتشار شبكتها حيث يمكن أن تتواجد أينما وجدت الإنارة .
- تعتبر صديقة للبيئة .
- استهلاكها القليل للطاقة .

ما هي الأشياء التي تنقصها ؟

- حزمة البث تكون موجّهة وتنتشر في مساحة محددة , لذلك يحتاج إلى أكثر من نقطة بث لتغطية المبنى .
- ضرورة أن يكون المجال مفتوحاً بين نقطة الإرسال والاستقبال، فعلياً يمكننا استقبال الإشارة عند قطع الفراغ بينهما نظراً لانعكاس الضوء وانكساره , ولكن يتوقف الاتصال عندما يتم تغطية المجال بين النقطتين بشكل تام .
- يحتاج الجهاز المستقبل إلى إضافة قطعة إلكترونية تمكّنه من إرسال واستقبال وفهم هذه الإشارات .

بقي أن أضيف بأنّ هذه التقنية يجري العمل عليها حالياً بشكل أساسي لتحسين سرعتها , ويتوقع أن يكون لها قبول وشعبية في المستقبل القريب، وكما يقول «هارالد هاس» أبرز الباحثين في هذا المجال والذي يعمل كأستاذ في معهد الاتصالات الرقمية في جامعة ادنبره في اسكتلنده « إنّ الاتصالات عبر الضوء المرئي ستؤدي إلى ارتباط أوثق بين البشر والآلات». وبهذا فهي ليست الأفضل في الوقت الحالي ولن تكون البديل لباقي الشبكات , ولكن حسب رأيي ستكون حل لبعض نقاط الضعف لتقنيات الشبكات الأخرى وإضافة جيدة لها. وكما قلت هذه التقنية هي الآن تحت الأبحاث والتجارب ومن المؤمّل أن تطبق تجارياً بشكل تجريبي في عام 2012 إن شاء الله.

الهجوم على الشبكات اللاسلكية

أحدثت الشبكات اللاسلكية طفرة في عالم الشبكات وأدت إلى ظهور تقنيات حديثة سهلت عملية التشبيك . كما أتاحت لنا هذه التقنية الإتصال بالشبكات أثناء التجوال. فقد أثارت هذه التقنية إهتمام المستخدمين والمؤسسات مما أدى ذلك إلى جذب الشركات لتطوير منتجات جديدة تستخدم الإتصال اللاسلكي . وسرعان ما إنجذبت الشركات فعل ذلك ، سرعان ما إنجذبت فئة أخرى لتستغل هذه التقنية ولكن بشكل معاكس . الآ وهي فئة الهاكرز .

من هم الهاكرز ؟

لاشك أنك سمعت عن الهاكرز مرراز وتكرارا.

ولا شك أنك سمعت عنهم فقط أنهم الفئة المخربة او المتجسسة على بينات المستخدمين .

ولكن الواقع مختلف عن ذلك . فهنالك 3 فئات من الهاكرز .

فئة ترتدي القبعة البيضاء ، وهي الفئة التي تسعى للإختراق من أجل الإختبار ومعرفة نقاط الضعف و تعلم سد الثغرات .

أما الفئة الثانية ، فهي الفئة التي ترتدي القبعة السوداء والتي تسعى دائماً لتخريب والتجسس على المعلومات.

وهنالك فئة ثالثة ترتدي القبعة الرمادية وتقع بين الفئتين السابقتان ، فتراة ما تخرب وتراة ما تسعى للحماية من خبرتها في الإختراق.

وما يهمنا ذكره هنا أن الهاكرز الحقيقي هو الذي يتمتع بخبرة في البرمجة وله القدرة على إنشاء وتطوير أدوات الإختراق. كما له القدرة على معرفة عمل الأنظمة .

بعد هذه المقدمة ، نفتح الباب لندخل في صلب الموضوع لنتعرف على الهجمات المستخدمة في إختراق الشبكات اللاسلكية .

كيف يتم الهجوم على الشبكات اللاسلكية ؟

تقوم الشبكات اللاسلكية ببث ونقل البيانات عبر موجات الراديو . وتسبح هذه البيانات في الهواء بإتجاه الجهة المرسلة لها . وتحتوى هذه البيانات السابحة في الهواء على معلومات عن الأجهزة المرسلة والمستقبلة .



بما أن البيانات السابحة في الهواء تحتوي على معلومات عن الشبكة ، خطرت فكرة على الهاكرز لإصطياد هذه البيانات أو أجزاء منها لتحليلها والإستفادة منها للهجوم على الشبكات . وبدأ الهاكرز بإستخدام أساليب مختلفة للحصول على أكبر قدر ممكن من المعلومات . فلديهم عدة أنواع من الإختراق سنتطرق على الأكثر شيوعاً منها :

النوع الأول : Network Sniffing

في هذا النوع من الإختراق ، يقوم المخترق بالتنصت على حركة مرور

البيانات وذلك بإستخدام برامج خاصة يطلق عليها Sniffers .

تقوم برامج Sniffing بالتنصت حركة مرور البيانات المرسلة والمستقبلة المنتقلة عبر موجات الراديو . حيث يقوم المخترق بإصطياد الـ packets أو رزم البيانات والتي تحتوي على Source IP أو عنوان المرسل و Destination IP أو عنوان المستقبل . و يستفيد المخترق من هذه العناوين في عملية الإختراق .



ويمكن للمخترق أيضاً إصطياد البيانات التي تحتوي على كلمات السر وذلك عندما يقوم المستخدم بالإتصال بالشبكة عن بعد . مثل إستخدام برنامج Telnet ، حيث تعبر كلمة السر ضمن البينات لتذهب للجهة الاخرى لتحقق منها ، فيستغل المخترق هنا الفرصة لإصطياد هذه البيانات وإستخراج كلمات السر منها.

النوع الثاني : MAC Spoofing

يعتمد هذا النوع من الإختراق على النوع السابق (Network Sniffing) . حيث يقوم المخترق بعملية تزوير الفريمات التي حصل عليها من عملية الـ Sniffing . ويتطلب هذا الإختراق عمل IP Spoofing تزوير عنوان IP وأيضا MAC Spoofing أي تزوير عنوان الـ MAC . وكما تعلم أن الـ Frames هي أجزاء من البيانات تحتوي على معلومات عن الشبكة والبروتوكولات ومنافذها وتحتوي أيضا على MAC Source الخاص بالجهاز المرسل و MAC Destination الخاص بالجهاز المستقبل وكذلك IP Source و IP Destination.

وبعد أن يقوم المخترق بالحصول على عناوين الـ MAC والـ IP، فإنه يستطيع خداع السيرفر والأجهزة الأخرى بإرسال فريمات مزورة تحتوي على عنوان أحد الأجهزة الموجودة على الشبكة بحيث تستقبل الأجهزة الاخرى كل شي منه دون شك . وبهذه الطريقة يستطيع المخترق التواصل مع أي جهاز على الشبكة .

النوع الثالث : WAR Driving

هذا النوع من الإختراقات فكرته التجول بسيارة مزودة بلاقط لاسلكي يستطيع إلتقاط الشبكات عن بعد . فيقوم المخترقيين بالبحث عن المناطق التي تكثر فيها الشبكات اللاسكلية ويقتربوا منها ليتمركزا في مكانا معين . ثم يبدءُ توجيه اللاقط الخاص به في عدة إتجاهات لإلتقاطات أكبر قدر ممكن من الشبكات اللاسلكية وبدء الهجوم عليها .



ولعمل إختراق من هذا النوع ، يتطلب على المخترق أن يكون متمكن ومتمرس في عمليات الهجوم والإختراق وذلك لأنه سيواجه شبكات كثيرة ذات حمايات وتشفير مختلف .

وختاماً في هذا المقال ، إننا نوصيك بالإمور التالية للتحسين من حماية شبكتك :

1 - وضع الـ Access Point الداخلي في مكان يبعد عن النافذة بحيث لا تتسرب الإشارة إلى الخارج .

2 - إستخدام أنواع تشفير قوية لحماية شبكتك اللاسلكية مثل WPA2-PSK بتشفير AES .

3 - وضع الإعدادت الصحية على Access Point والتي لها الدور في زيادة مستوى الحماية مثل MAC Filtering التي تسمح للمستخدمين المسجل عنوان MAC الخاص بهم دخول الشبكة .

4 - إستخدام بروتوكالات ذات تشفير قوي لعمل إتصال عن بعد أو لنقل البيانات ، مثل بورتوكول SSH .

5 - تركيب أجهزة كشف ومنع الإختراق مثل WIDS .

NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية













DNS ???

ما هو الـ DNS ؟؟؟

Identification
علاء معن الشوا
الجنسية : سورية
مهندس إلكترون
قسم تحكم آلي وأتمتة صناعية ومقبل على علم شبكات الحاسب
alaashawwa@hotmail.com
SYRIA

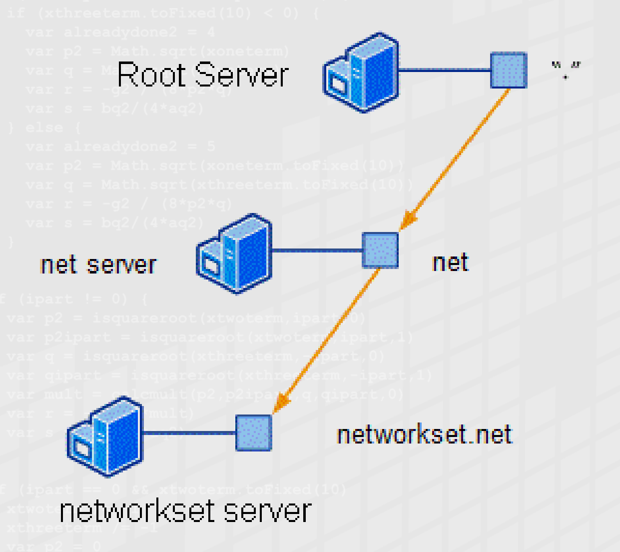
الكثير منا في هذه الأيام يجد صعوبة في حفظ أسماء مواقع أو روابط الإنترنت التي يتعامل بها يوميا، فنجد من يستخدم أحد محركات البحث أو قائمة المفضلة للوصل إلى المواقع المرغوبة، ولكن تخيل عزيزي القارئ لو أخبرتك بأن هذه الأسماء ليست هي حقيقة ما يتم التعامل معه عبر شبكة الويب الضخمة والتي تحوي الملايين من المواقع، وإنما هذه الأسماء هي عبارة عن عناوين (IP) يتم تحويلها باستخدام الـ DNS:) (Domain Name System للوصول إلى تلك المواقع، بالمحصلة هو عبارة عن نظام يحوي قاعدة بيانات موزعة على الإنترنت وظيفتها ترجمة أسماء النطاقات من أسماء إلى أرقام تعرف باسم (IP Address)

ظهور فكرة الـ (DNS) ....

عندما قام مصممو بروتوكول الـ (TCP/IP) بوضع وبناء هذا المفهوم، ظهرت الحاجة لتعريف كل جهاز ضمن هذه الشبكة التي يتم التعامل معها، لذلك قاموا بوضع رقم يقوم بتحديد موقع وتوضع كل جهاز وفق معايير أساسية عامة والذي هو متداول لدينا باسم الـ (IP)، لكن ذلك أدى إلى ظهور مشكلة أخرى عند استخدام الأشخاص العاديين أو قليلي الخبرة في هذا المجال، فكان عليهم تذكر الـ (IP) الخاص بكل جهاز موجود على الشبكة، إضافة إلى الانتشار الواسع الذي حققته شبكة الويب ووجود الآلاف أو ربما عشرات الآلاف من المواقع حينها ....كل هذا وأكثر دفع مصممو الشبكات لايجاد طريقة تقوم بتسهيل الوصول إلى الجهاز الهدف وبطريقة تكون سهلة الحفظ والتذكر من قبل المستخدم، فظهرت فكرة ربط الـ (IP) الخاص بموقع أو مخدم ما إلى اسم يدل على هذا الموقع أو الغرض الذي أنشئ من أجله، وبناء على ذلك تم إيجاد الـ (DNS) ليقوم بترجمة الاسم المطلوب إلى الـ (IP) الموافق له.

آلية عمل الـ DNS :

ترتكز آلية عمل الـ (DNS) في حل الأسماء وترجمتها على التسلسل الهرمي، فلو أخذنا مثالا بسيطا لجهاز متصل بشبكة الإنترنت وطلب موقع www.networkset.net فإن المخدم المحلي سيقوم بتحديد فيما اذا كان يوجد تحليل أو ترجمة (والمقصود هنا IP للموقع networkset.net) للوصول إلى منطقة المخدم المطلوب أم لا.
اذا لم يجد المخدم المحلي تطابق للاسم المطلوب



فسوف يمرر الطلب إلى مخدم ذو مستوى أعلى والذي هو الـ (Root Server) ومن ثم ستتكرر العملية نفسها في الـ (Root Server) فان لم يجد تطابق للموقع المطلوب يقوم بتمرير الطلب لمخدم الـ com وتستمر العملية في التكرار حتى نصل إلى المخدم المطلوب والذي هو في مثالنا (Networkset) ....
الآن في حال إعادة طلب نفس الموقع من جهاز آخر في الشبكة المحلية، سيعطي حينها المخدم المحلي تطابق للطلب (networkset.net) وذلك لان السيرفر المحلي يقوم بحفظ جميع ترجمات المواقع التي تم طلبها لديه ولمدة زمنية يحددها مسؤول المخدم.

مكونات نظام الـ (DNS) :

نستعرض هنا المكونات وفق التسلسل الذي قامت بتصميمه شركة مايكروسوفت في أنظمة السيرفر الخاصة بها:

1 - اسم النطاق أو ما يعرف بـ (Domain Name) وهو عبارة عن اسم (string) ليس له أي دلالة برمجية ولكن يستخدم للإشارة إلى اسم المؤسسة أو المنظمة على شبكة الإنترنت

2 - ملف النطاق أو (Zone File) وهو عبارة عن ملف يحوي المعلومات والإعدادات الخاصة بنطاق معين، ويمكن التعديل عليه من قبل مسؤول المخدم

3 - مخدم اسم النطاق (Domain Name Server) وهو عبارة عن مخدم او أكثر يقوم بالرد على الطلبات المرسلة من قبل المستخدمين وفقا لما هو موجود في ملف النطاق، ويشترط وجود مخدم واحد على الأقل يمتلك لملف النطاق، وتتم بقية المخدمات في حال وجودها عمل المخدم الرئيسي من خلال أخذ نسخة من ملف النطاق

4 - المخدم المحلل (Resolver Server) وهو عبارة عن مخدم يوجد ضمن كل شبكة محلية يقوم بتخزين طلبات المستخدمين وإيجاد التحليل أو الترجمة لطلبات تلك الأجهزة، ويتم ذلك عن طريق الاتصال بمخدمات أسماء النطاق حيث يقوم بعدها (كما ذكرنا سابقا) بالاحتفاظ بالنتائج لمدة معينة يحددها مسؤول المخدم، ويتم ضبط تلك الزمنية من خلال البيانات الموجودة ضمن ملف النطاق

5 - المستخدم أو الزبون (client) وهو المستخدم العادي الذي يقوم بارسال الطلبات ويستقبل النتائج وفقا لتسلسل العملية السابقة، أي هو الطرف النهائي لهذا النظام.

في النهاية أريد أن أشير إلى أن بعض المواقع التي يتم طلبها بشكل كبير جدا تمتلك أكثر من مخدم موزعة على مناطق جغرافية محددة وكل مخدم يمتلك عنوان (IP) خاص به، أي في المحصلة يوجد أكثر من (IP) للموقع ذاته وعلى النقيض تماما بعض المخدمات تحتوي على أكثر من موقع ويب ولها عنوان (IP) وحيد ،هنا يبرز دور الـ (DNS) مع عوامل أخرى تساعد المستخدم العادي إلى تلبية طلبه للموقع المرغوب دون حدوث أي تضارب أو خطأ أثناء عملية الاتصال.





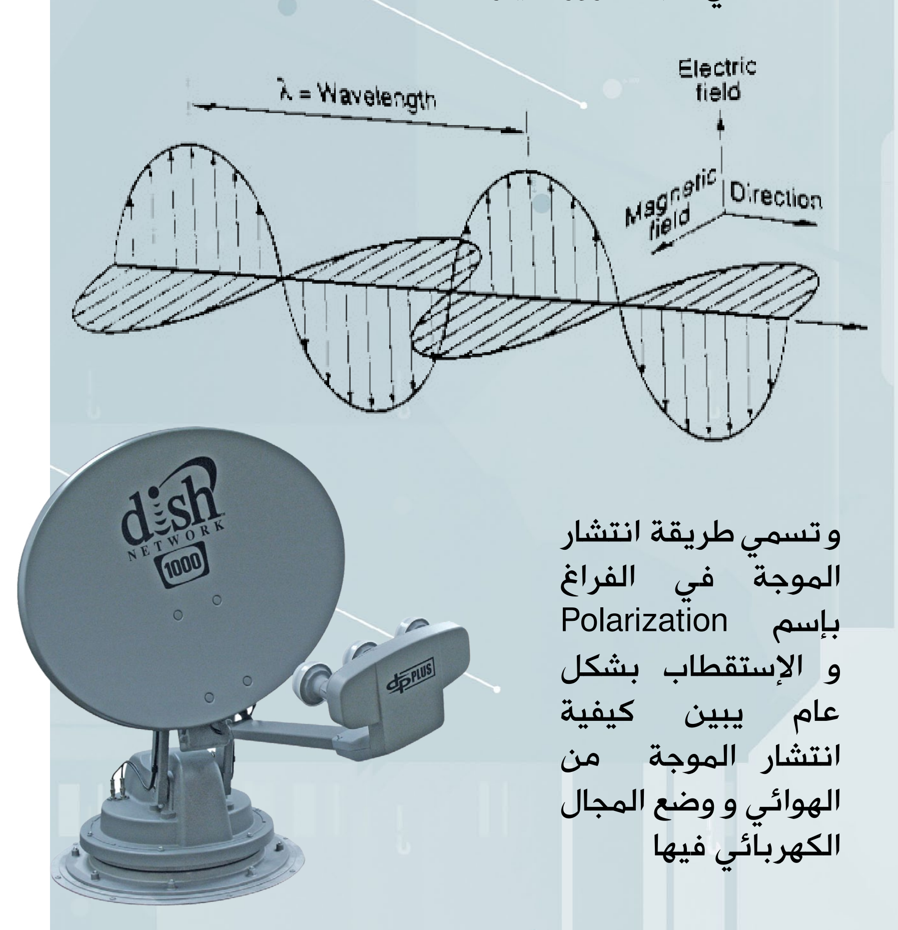
عادت قناة الناس الدينية للبث باستقطاب أفقي علي التردد 11919

لعلك فرحت يومها مثلي بهذا الخبر و قمت سريعا بإضافة باقة بتردد 11919 مع اختيار H في خانة الإستقطاب لكن ألم تفكر بكونك مهندس شبكات ما المقصود بكلمة استقطاب أفقي Horizontal Polarization هذه المصطلحات لا يختلف معناها هنا عن معناها في الشبكات اللاسلكية أو في أي منظومة لاسلكية و لابد أن تعرف ما المقصود بها ان كنت مهتما بالشبكات اللاسلكية أو علي الأقل عند شرائك لأجهزة تقوية الشبكات اللاسلكية

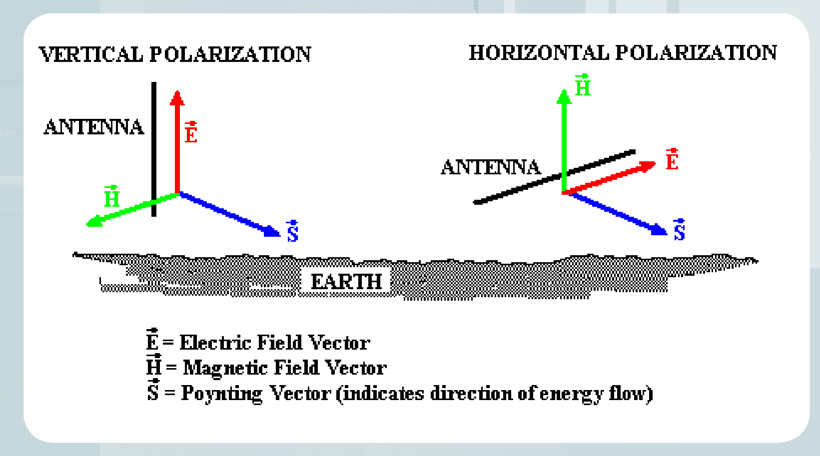
و الهوائيات أو الإريال تعتبر من أهم أجزاء أجهزة الإرسال و الإستقبال فبدونها لن يستطيع الجهاز بث أو استقبال الإشارة الا لمسافة أمتار قليلة و تعتمد عليه كل أجهزة الإرسال و الإستقبال مثل الأكسس بوينت في الشبكات اللاسلكية و الهواتف الخلوية و الأقمار الصناعية
و اجهزة الراديو و التلفاز و غيرها
و هي جزء كهربي معدني يقع في نهاية الدائرة الإلكترونية للأجهزة الإلكترونية المتخصصة في الإرسال أو الإستقبال و يقوم بتحويل التيار الكهربائي الي موجات راديوية و ذلك في أجهزة الإرسال و يقوم بتحويل الموجات الراديوية الي كهربية في أجهزة الإستقبال

و يعتبر أول هوائي تم استخدامه و تصنيعه في عام 1888 بواسطة العالم هرتز في معمله ليثبت وجود الموجات الكهرومغناطيسية التي تحدث عنها العالم ماكسويل في نظريته

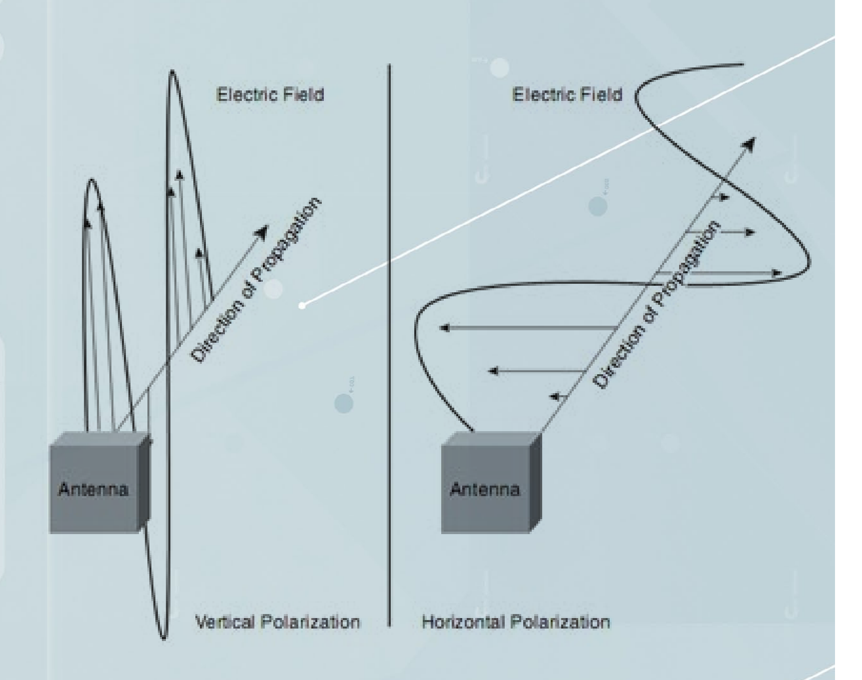
الهدف من الهوائيات كما قلنا هو الإشعاع الكهرومغناطيسي و الذي يتكون من جزئين متعامدين تكونهما كلمة «كهرومغناطيسية» و هما جزء كهربي يمثل الموجة متعامدة مع جزء مغناطيسي
و ينشأ المجال الكهربائي بواسطة شحنات كهربية وعند تحرك هذه الشحنات ينتج التيار و الذي بدوره ينتج مجال مغناطيسي متعامدة علي اتجاه مرور التيار



و تسمي طريقة انتشار الموجة في الفراغ بإسم Polarization و الإستقطاب بشكل عام يبين كيفية انتشار الموجة من الهوائي و وضع المجال الكهربائي فيها

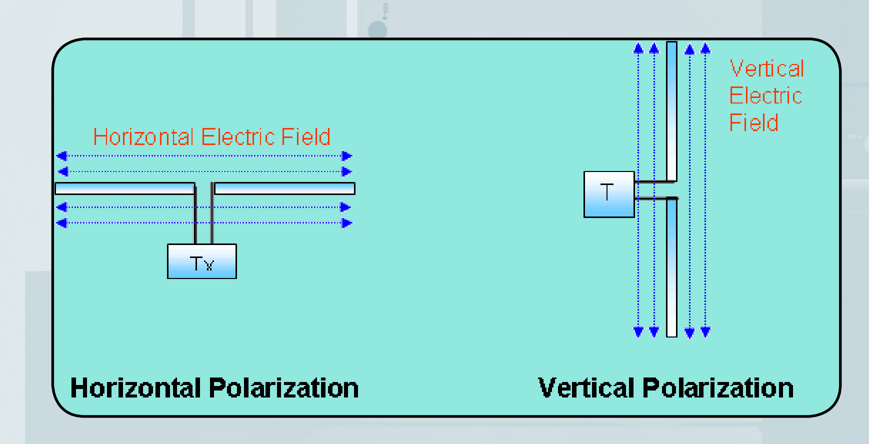


و الموجة تنتشر خطيا أو كرويا أو بشكل بيضاوي
فأما الإنتشار الخطي وهو المهم عندنا في الشبكات اللاسلكية فينقسم الي نوعين
Vertiacl
Horizontal
و كما تري في الشكل فإن Vertical Polarization يعني أن الموجة تنتشر في الفراغ في شكل خطي ارتفاعا و انخفاضا أما Horizontal Polarization فيعني أن الموجة تنتشر في شكل خطي و لكن مع تذبذبها يمينا و يسارا

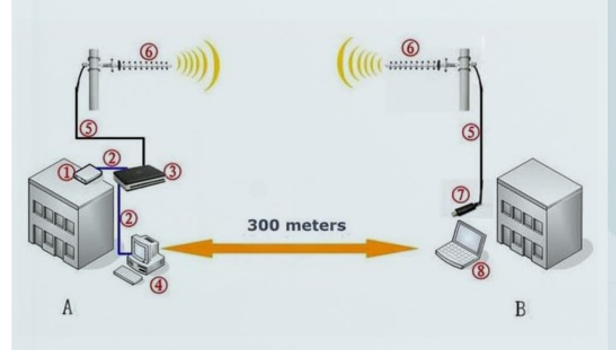


و قد بدأ استخدام الوضع الأفقي للهوائيات في عام 1950 حيث بدأ البث الأول للتلفاز في USA و لتلافي التداخل الذي سينشأ عن وجود ناطحات السحاب فقد قام المصممون بعمل هوائيات التلفاز ذو استقطاب أفقي

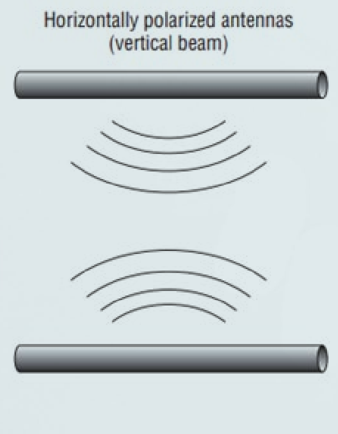
وعند بداية عصر شبكات نقل البيانات تم عمل استقطاب هوائياتها بشكل رأسي كي لا تتداخل مع الموجات المستقطبة رأسيا من هوائيات التلفاز و ذلك تجد ان كافة هوائيات أبراج الموبايل استقطابها بشكل رأسي

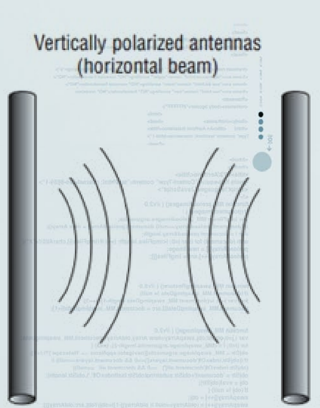


وعند شرائك للهوائي ستعرف وضع الإستقطاب الذي صمم من أجله و غالبا و كماتقول سيسكو فإن كل هوائياتها رأسية الإستقطاب Vertical Polarized
و لذلك فإنه غالبا لن تجد هوائي من سيسكو موضوع بشكل أفقي خصوصا في الشبكات الخارجية outdoor
و هذا لا يعني اطلاقا أن كل الهوائيات من الشركات الأخري ذات استقطاب رأسي و لكن سيسكو تفضل ذلك و أمامك صورة لشبكة لاسلكية خارجية تستخدم هوائي yagi موضوع بشكل استقطاب أفقي



و الهوائي السابق قابل لوضع في شكل رأسي أيضا حسب ما ذكرت وثائقه المرفقة معه و لكن لابد أن يكون كل من الهوائيين في المرسل و المستقبل في وضع استقطاب متشابه و الا فإنك ستعاني من فقد كبير في الطاقة عند الإستقبال

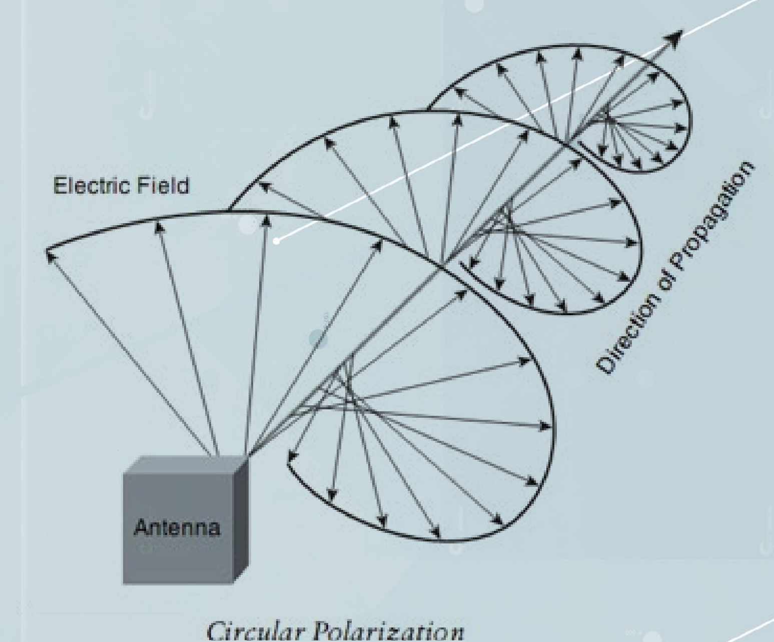






أما في الشبكات اللاسلكية الداخلية فإن انعكاسات الموجة كثيرا علي الجدران يغير من حالة استقطاب الموجة مما يجعل وضع استقطاب الهوائي غير مؤثر

هذان النوعان السابقان من الإستقطاب كما قلنا يسميان الإستقطاب الخطي حيث تسير الموجة في اتجاه خطي واحد و هناك نوعان آخران أولهما هو الإستقطاب الكروي Circular Polarization و الذي يعني أن الموجة تنتشر بشكل غير خطي كما تري



Circular Polarization



يستخدم هذا الإستقطاب في أجهزة الإستقبال من الأقمار الصناعية حيث لا يهم أن يكون الإستقطاب افقي أو رأسي فالهوائي سيكون قادرا علي استقبال النوعين فأنت عندما تختار نوع استقطاب الباقة الترددية في أجهزة الريسيفر لا يهمك وضع هوائي الإستقبال أثناء وضعك للباقة لأن وضعه الأصلي لإستقبال باقات القمر كافي لإستقبال أي استقطاب

أما النوع الأخير من الإستقطاب فيسمي Elliptical Polarization و هو حالة وسط بين الإستقطاب الخطي و الإستقطاب الكروي

كيفية الحصول على أيبي شبه حقيقي وربطه مع أجهزة سيسكو.

Identification
أيمن النعيمي
الجنسية : سورية
مهندس شبكات سوري مؤسس أول مجلة وموسوعة عربية في الشبكات حائز على عدة شهادات علمية ومهتم بالمحتوى العربي على الأنترنت
admin@networkset.net
SYRIA

يعتبر حجز أيبي حقيقي من مقدمي الخدمة أحيانا شيئ باهظ الثمن وأحيانا غير متاح ابدا , ولحل هذه المشكلة سوف نلجأ إلى أحد الخدمات القديمة المتوفرة بشكل مجاني على الأنترنت والتى سوف تعطينا نفس خواص الأيبي الحقيقي لكن من خلال استخدامنا للديناميك أيبي الذي يزودنا به مقدم الخدمة , وسوف تفيدنا هذه الخاصية في الأتصال عن بعد بالروترات والاجهزة الموجودة على الانترنت من أي مكان آخر بألأضافة إلى أتاحة تنفيذ عملية ربط بين فروع الشركات من خلال تقنية الـ VPN

فكرة الخدمة .

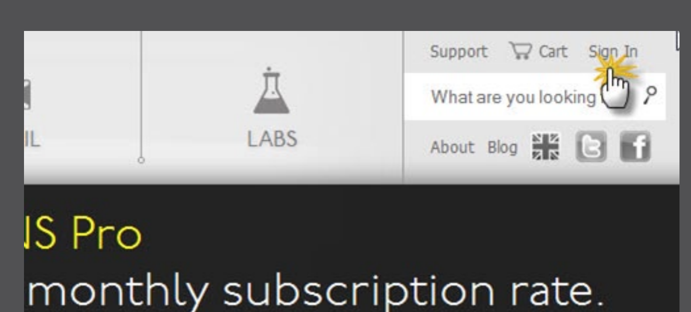
تعتمد فكرة الموقع على مبدأ إعطائك عنوان أو هوست يكون عادة على الشكل الآتي test.dyndns.org ويكون البديل الرسمي للريل أيبي وهي خدمة مجانية محدودة نوعا ما تسمح لك بالحصول على



عنوانان فقط ولو رغبت بالحصول على أيبيات أكثر يتوجب عليك أن تسجل مرة آخرى , فكرة الربط بين الأيبي المتغير لديك والهوست الخاص بالموقع بسيطة جدا فلو كنت تعتمد على الهاردوير في عملية الربط بين الفروع فالجهاز بنفسه يتكفل بأرسال الأيبي الخاص بك والحالي إلى موقع الـ DynDNS ويخبرهم أن هذا الهوست عنوانه الحالي كذا , وبالتالي يخزن الموقع الأيبي الخاص بك ويربطه بالهوست نايم الذي أخترته وهو في مثالنا test.dyndns.org فلو صادف أن هناك من يريد الأرتباط معك فسوف يكون عنوانك الثابت ليس أيبي بل هوست والموقع هو من يتكفل بعملية الترجمة من الأسم إلى الأيبي وفي كل مرة يتغير الأيبي لديك يرسل الجهاز الأيبي الجديد إلى موقع الـ DunDNS ويخبرهم بالتغيير ومباشرة يقوم الموقع بتحديث قاعدة البيانات الخاصة به ويحدث عملية الربط بين الهوست والأيبي , اما لو كان الربط بين الفروع من خلال السوفت وير أي VPN Software فنحن في هذه الحالة نحتاج إلى برنامج صغير نركبه على أحد الاجهزة الموجودة على الشبكة بشرط ان يكون الجهاز مربوط مع الأنترنت وهو يتكفل بعملية التواصل مع الموقع ويخبره بكافة التغييرات بشكل أوتوماتيكي .

مراحل التسجيل

الدخول إلى رابط الموقع /http://dyn.com



وبعدها نملا الفراغات بالمعلومات المطلوبة , ونعلم على صندوق الأتفاقية مع الموقع

Username networkset
Password ••••••••
Confirm password ••••••••
Email networkset@hotmail.com
Confirm Email networkset@hotmail.com
Security Image 6 4 4 0 3
Enter the numbers from the above image:
64403
Subscribe to DynDNS.com newsletter (One or two per
I accept the terms of Dyn's Acceptable Use Policy, the
Policy.
Create Account
If you're having difficulty creating your account, for any reason, feel free to conta

وبعدها سوف تصلك رسالة تفعيل إلى البريد لتأكيد الحساب تضغط عليه فتعود مرة آخرى للموقع وتقوم بكتابة كلمة السر

lease log in to finalize account activation.
Username networkset
Password ••••••••
Confirm Account
Forgot your password?

الخطوة التالية هي أضافة هوست للحساب ونبدأها بالدخول إلى الحساب من خلال My Account

Welcome networkset FREE My Account My Cart Log Out

وبعدها نختار Add Host

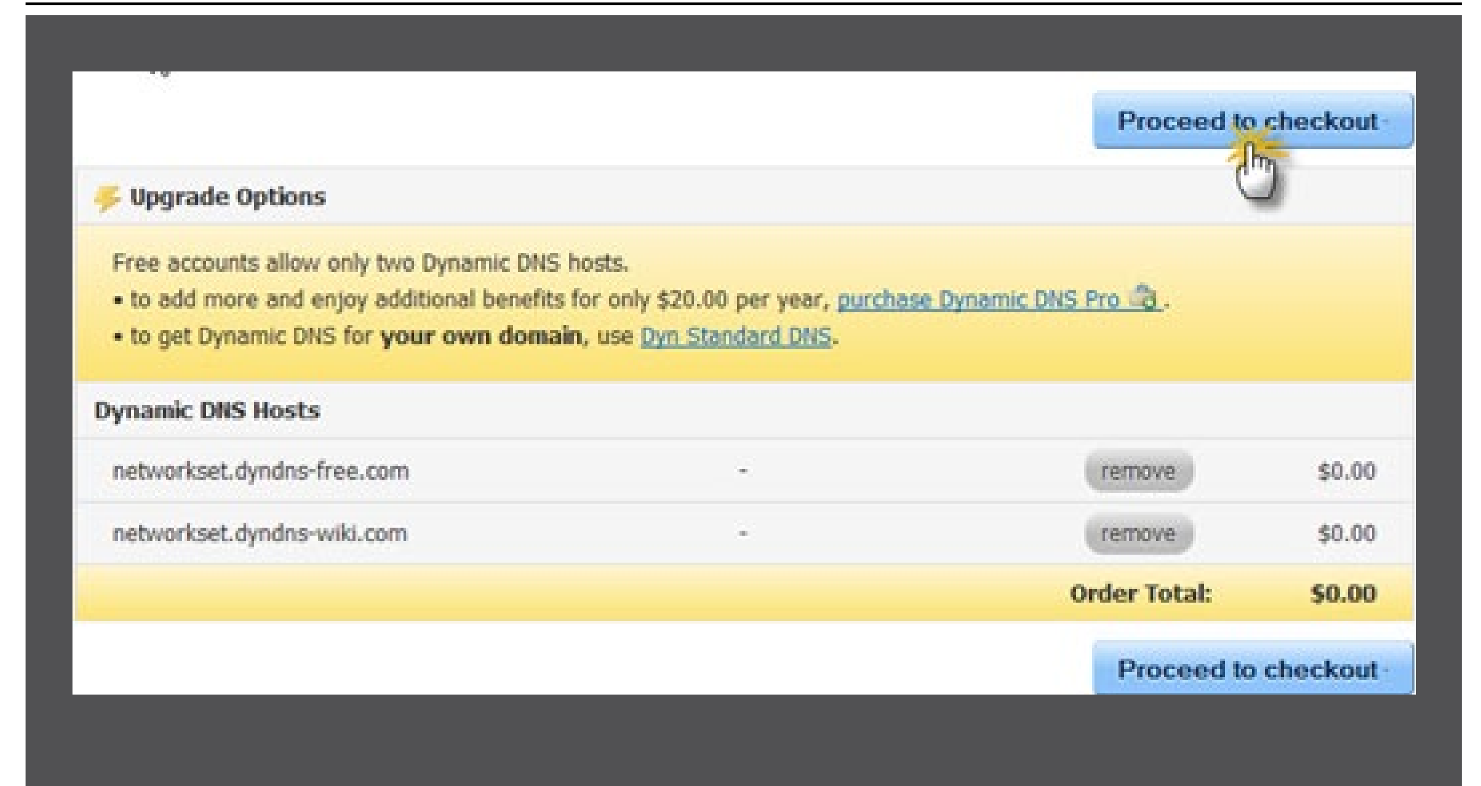
My Services
View, modify, purchase, and delete your services.
My Zones/Domains
Add Zone/Domain Services
My Hosts
Add Host Services
Dynamic DNS Pro
DynECT Managed DNS Lite
Internet Guide
Dyn Standard SMTP
Support
Premier Support
Contact Support

Billing
Update your billing information, complete a purchase, and view invoices.
View Shopping Cart
Active Services
Order History
Billing Profile and Vouchers
Renew Services
Auto Renew Settings
Sync Expirations

وخطوتنا القادمة هي أهم خطوة , نقوم أولا بأختيار أول جزء من الأسم وعادة مانختاره بحيث يناسب موقع الربط أو موقع الفرع حتى يسهل علينا التعرف عله وفي مثالي أخترت NetworkSet وبعدها نختار Host with IP Address الخيارات الباقية واضحة ومفهومة , الخطوة الثالثة غير الزامية لأن الروتر أو البرنامج سوف يرسل الأيبي للموقع لأحقا , لكن بشكل عام أكتبه كما يشير الموقع إلى الأيبي الخاص بك الآن .

Hostname: networkset . dyndns-wiki.com
Wildcard: create "*.host.dyndns-yourdomain.com" alias (for example to use same settings for www.host.dyndns-yourdomain.com)
only for DynDNS Pro users
Service Type: Host with IP address
WebHop Redirect (URL forwarding service)
Offline Hostname
IP Address: 178.152.
Your current location's IP address is 178.152.
IPv6 Address (optional):
TTL value is 60 seconds. Edit TTL...
Mail Routing: I have mail server with another name and would like to add MX hostname...
Add To Cart

وبعدها تابع معي بالصور



Once you have confirmed the contents of your cart your services will be instantly activated.

Service	Price
Dynamic DNS Hosts	
networkset.dyndns-free.com	$0.00
networkset.dyndns-wiki.com	$0.00
Order Total:	**FREE**

Activate Services

Host Services

↑ My Services

2 hosts activated.

Hostname	Service	Details	Last Updated
networkset.dyndns-free.com	Host	178.152.	Oct. 20, 2011 10:50 AM
networkset.dyndns-wiki.com	Host	178.152.	Oct. 20, 2011 10:50 AM

» Host Update Logs
» Bulk Update IP Address And Service Type

Add New Host

كما نشاهد في الصورة الآخيرة أضفت عنوانان أثنان لأستخدمهم في عملية الربط ويشير الموقع إلى أن الخدمة مفعلة والعناوين جاهزة للربط , وكون الحساب من النوع المجاني فنحن لانستطيع أن نضيف أكثر من أثنان هوست وهم كافيين لتمكيننا من ربط فرعان ببعضهما البعض .

ربط الأيبي مع أجهزة سيسكو

بعد حصولنا على أيبي شبه حقيقي من موقع DynDNS نتوجه الآن إلى روتر سيسكو لنقوم بأعداده بحيث يقوم بتحديث قاعدة بيانات الموقع بشكل مباشر ودائم وبدون تدخل من أحد , الأيبي عادة يكون على الشكل الآتي networkset.dyndns-free.com وهو لن ينفعنا الآن ولن نستفيد منه بشيئ طالما لم نستخدمه في ربط الفروع ببعضها لكن مفيد لو في حال قررنا الاتصال بالروتر عن بعد , نتوجه إلى الروتر وندخل إلى الـ Configuriton Mode وننفذ الأوامر التالية :

```
Router(config)#ip ddns update method Dyn_IP
Router(DDNS-update-method)#http
Router(DDNS-HTTP)#add http://username:password@members.dyndns.org/nic/upda
te?system=dyndns&hostname<h>&myip=<a>
Router(DDNS-HTTP)#exit
Router(DDNS-update-method)#interval maximum 14 0 0 0
Router(DDNS-update-method)#exit
```

بالنسبة للأوامر وتفسيرها : الأول أمر ثابت من أجل أعداد الـ Method الذي سوف نعده من أجل تطبيقه فيما بعد على المنفذ ولاحظ أن كلمة Dyn_IP هي أختيارية وتستطيع كتابة ماتريد لكن يجب تذكرها , الأمر الثاني من أجل تحددد البروتوكول الذي سوف نستخدمه في عملية التحديث مع موقع الـ ر DynDNS , الأمر الثالث وهو صيغة ثابتة مأخوذة من موقع DynDNS
نقوم بتغيير أسم المستخدم وكلمة السر الخاصة بنا في الموقع ولاننسى أضافة كلمة ADD قبل الصيغة كما هو موضح في الأمر .

```
http://username:password@members.dyndns.org/nic/update?system=dyndns&hostn
ame<h>&myip=<a>
```

ملاحظة في غاية الخطورة : لاحظوا أشارة الاستفام الموجودة بين كلمة update و system لو في حال قمت بنسخ الأمركما هو والصقته في محرر الأوامر فأن أشارة الأستفام لن تظهر كونها مرتبطة بوظيفة خاصة في نظام التشغيل (عرض المساعدة) والحل هو أن تقوم أولا بالضغط على زر الكونترول زائد حرف الـ V مرة واحدة وبعدها أطبع أشارة الأستفهام

الأمر الرابع من أجل أعداد المدة الزمنية القصوى التى سوف يبقى الروتر لايحدث فيها قاعدة بيانات الموقع , وبكلام آخر قد يبقى الروتر يعمل مدة طويلة قد تستمر لأشهر وهو في هذه الحالة لايحتاج إلى تحديث قاعدة البيانات في الموقع لكن قد تحدث اسباب تؤدي إلى تغيير الأيبي في الروتر من دون عمل أعادة أقلاع للروتر لذلك نحدد مدة زمنية نخبر فيها الروتر أن يقوم بالتحديث بعد أنقضاء هذه المدة وهي تبدأ بالأيام والساعات والدقائق والثواني .
بعد أن ننتهي نتوجه إلى المنفذ المتصل مع الأنترنت وهو عادة مايكون منفذ الـ Dialer ونقوم بتنفيذ الأوامر التالي وهي واضحة ولاتحتاج إل تفسير

```
Router(config)#interface Dialer0
Router(config-if)#ip ddns update hostname networkset.dyndns-free.com
Router(config-if)#ip ddns update Dyn_IP
```

وبهذا نكون قد انتهينا من أعداد الروتر بحيث يقوم بشكل أوتماتيكي بتحديث قاعدة بيانات الموقع وبدون الحاجة إلى تنصيب اي برامج آخرى داخل الشبكة وخطوتنا القادمة سوف تكون خاصة بتنصيب البرنامج المخصص لي DynDNS لتحديث الأيبي من خلال ويندوز وطبعا البرنامج مفيد لو في حال كنت تعتمد على حلول VPN Software في ربط بعض الفروع ببعضها البعض أو تستخدم خدمات تحتاج أيبي حقيقي مثل الـ Exchange Server , إنتظرونا في العدد القادم مع طريقة تفعيل وربط الفروع ببعضها البعض من خلال تقنية الـ VPN .

BASECONFIG



مع التطوير المستمر لبرنامج الـ GNS3، وتسهيلاً على الدارسين بدأ ظهور ملف الـ baseconfig.txt في ملفات التثبيت الخاصة بالبرنامج في هذا المسار (C:\Program Files\GNS3\ directory)، بدءاً من النسخة 0.7.3 وهو يحتوي على عدة أوامر تسهل عملية إنشاء الـ Lab، عن طريق إعطاء الـ Router بعض الأوامر الأساسية التي تشترك فيها جميع الأجهزة في الـ Lab .

أسباب تطوير هذا الملف :

في البداية ما هي محتويات هذا الملف؟ :

```
!
hostname %h
no ip domain lookup
line con 0
exec-timeout 0 0
logging synchronous
```

- قبل النسخة 0.7.3 وعند إضافة أكثر من راوتر مثلاً في الـ Lab، كان يتم إعطاء نفس الاسم لكل الراوترات في الـ Console وهو ROUTER, ولكن مع الأمر الأول يتم إعطاء كل راوتر اسم مختلف وهو R1, R2, R3, .

2- في بعض الأحيان وعند كتابة كلمة خطأ مثلاً في الـ Console، فإنّ الـ Router يعتبر هذه الكلمة اسم لـ Host معيّن، ولكنّه لا يعرف هذا الـ Host لذلك يحاول أن يبحث عن IP لهذا الـ Host عنده, عن طريق البحث عن IP لـ DNS سيرفير تم تعريفه على الـ Router عن طريق الأمر

```
R# ip domain lookup
```

إذا لم يجده يقوم بعمل Broadcast ليبحث عن IP لهذا الـ Host، هذه العملية تؤدّي إلى حدوث Freeze للـ Console، وتظهر هذه الرسالة :

```
Router#xyz
Translating «xyz»...domain server (255.255.255.255)
 (255.255.255.255)
Translating «xyz»...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#
```

ولتفادي هذه المشكلة، يتم تعطيل هذه الخاصيّة بالأمر التالي :

```
no ip domain lookup
```

- أثناء الـ Lab، يتم إغلاق الـ Console بعد 10 دقائق في حال عدم كتابة أي شيء في الـ Console، ولكن مع هذا الأمر يتم تعطيل هذه الخاصية :

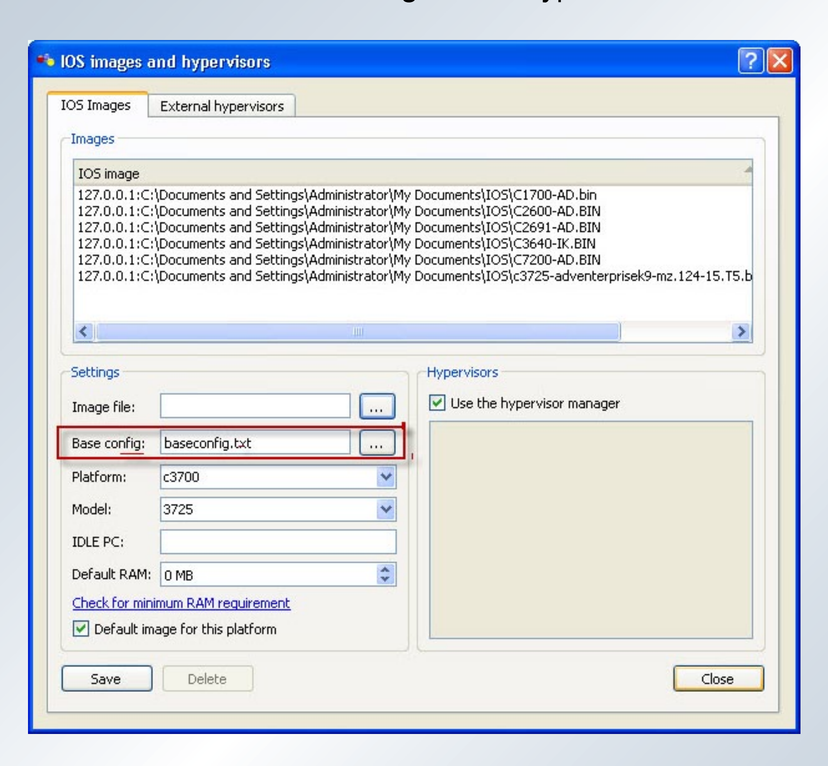
```
exec-timeout 0 0
```

أثناء الدخول على الـ Router من خلال الـ Console، وعند كتابة أي أمر فإنّ هذه الأوامر تتداخل مع الرسائل التي تظهر على الشاشةوهذا الأمر يجعل الأوامر تظهر في سطر بمفردها دون تداخل مع الرسائل التي تظهر :

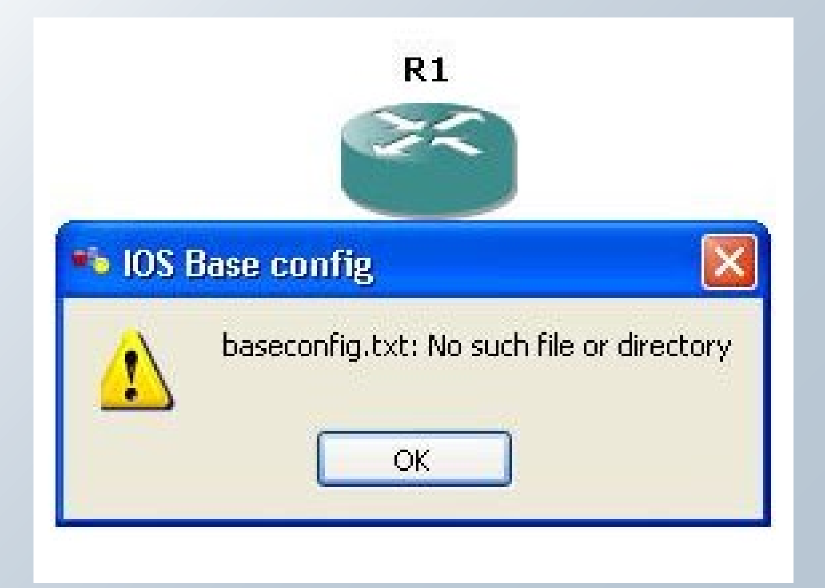
```
logging synchronous
```

هذه الأوامر كما أسلفنا توجد في ملف baseconfig.txt في مسار البرنامج، ويمكن إضافة أي أوامر أخرى ليتم تنفيذها على جميع الراوترات في أي Lab أخر، ويمكن تحديد هذه الأوامر وتغييرها من النافذة التالية :

Gns3>>Edit>>IOS images and hypervisors>>



وعند حدوث مشكلة في هذا الملف تظهر الرسالة التالية:



ولتفادي هذه المشكلة من الأفضل إعادة تثبيت البرنامج من جديد، أو عمل ملف بنفس الاسم في مسار البرنامج وكتابة الأوامرالسابقة فيه.

ولا تنسوني والمسلمين من صالح الدعاء وصلى اللّه وسلم وبارك على المصطفى وآله وصحبه وإخوانه وسلم.



Identification
أنس المبروكي
الجنسية : المغرب
23 سنة، مهندس في الشبكات والأنظمة
(EMSI- Rabat)
CCNA R&S ,CCNP R&S
mabroukianas@gmail.com
MOROCCO

يتكون الإنترنت من مئات الآلاف من شبكات الـ IPv4 والملايين من الـ IPv4 nodes . لكن تم تقريباً استهلاك جميع الـIPv4 addresses , وهو ما أدّى إلى اختراع الـ IPv6 الذي ضمن لنا العديد من العناوين. لكن كما هو معروف يعتمد نجاح أي تكنولوجيا جديدة على سهولة تكاملها واندماجها مع البنية التحتية القائمة دون انقطاع كبير في الخدمات. لحسن الحظ، فإنّ الانتقال من IPv4 إلى IPv6 لا يتطلب ترقيات على كافة الـ Nodes في نفس الوقت، بحيث أن الـ IPv4 و الـ IPv6 سوف يتواجدان معاً لفترة طويلة , بعد انتهاء هذه المرحلة سنحصل على شبكة مئة في مئة من IPv6 إن شاء اللّه. سأحاول في هذا المقال التحدث عن التقنيات التي تمكننا من الانتقال السلس من الـ IPv4 إلى الـ IPv6 وكيفية عملها .

هناك العديد من التقنيات المتاحة للانتقال بين IPv4 و IPv6 ويمكن تصنيف هذه الأساليب في الفئات الثلاث التالية :

- تقنية الـDual Stack : تقوم أجهزة الشبكة باستعمال كل منIPv4 و IPv6 في نفس الوقت. هذه التقنية مفيدة كمرحلة انتقالية مؤقتة، ولكنّها تضيف الحمل (Overhead) وتستخدم الكثير من الموارد (Ressources) .
- تقنية الـTunneling : يتم توصيل شبكات الـ IPv6 المعزولة عبر البنية التحتية لشبكات الـ IPv4 باستخدام الـ Tunnels. أجهزة الـ Edge هي الوحيدة التي تحتاج إلى استخدام الـ Dual stack .
- تقنية الـTranslation Protocol NAT : تستخدم جهاز يقوم بترجمة (Translation) الـ IPv6 packets إلى IPv4 Packets وبالعكس، وتسمح هذه التقنية للأجهزة التي تستعمل الـ IPv6 فقط على التواصل مع الأجهزة التي تستعمل الـ IPv4 فقط.

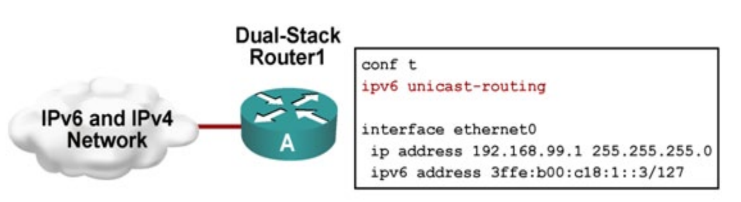
في الفقرة التالية سأتكلم عن كل هذه التقنيات بشكل مستفيض.

1. IPv4/IPv6 Dual Stacks :

يقوم الـ host باستخدام IPv4 وIPv6 address بالنسبة لكل كارت شبكةNIC . ليتمكن من إرسال حزم IPv4 إلى الـIPv4 hosts ، و إرسال حزم IPv6 إلى الـIPv6 hosts . أما فيما يخص الروتر, فبالإضافة إلى استعماله IPv4 addresses وبروتوكولات IPv4 routing ، فإنّه يستعمل IPv6 addresses و بروتوكولات IPv6 routing لدعم كل من IPv4 و IPv6 hosts ، إذ يمكن للروتر عمل Forwardلحزم IPv4 و لحزم IPv6 .

الـ Dual satck node يختار أيstack سيخدم استناداً للـDestination address ، ويفضّل إصدار IPv6 عندما يكون متاح.

كل روتر مُعد لعمل forward للـ IPv4 و الـ IPv6 يسمى dual stack router كما يوضّح الرسم أسفله ، هذا يعمل بشكل جيد، لكن يتطلب إعداد الـ IPv6 على جميع الروترات و التي في يوم ما ستتلقى حزمة IPv6 وسيتعيّن عليها توجيهها. بدلاً من ذلك ، قد يكون استخدام الـ Tunnels معقول لدعم عدد صغير من حزم الـIPv6 ، لأنّ الـ Tunnels تتطلب إعداد عدد أقل من الروترات في الـ IPv6.




```
conf t
ipv6 unicast-routing

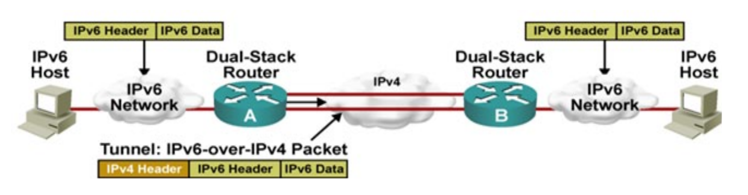
interface ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 3ffe:b00:c18:1::3/127
```

Dual-Stack Router

من عيوب الـ Dual Stack هي الموارد المطلوبة داخل كل جهاز مُعد بكِلا البروتوكولين . يجب على كل روتر تكوين الَـ routing table الخاص بكل بروتوكول ، الـToplogy table ، وهكذا دواليك ، ويجب معالجة كل بروتوكول بشكل مستقل. هناك أيضاً ارتفاع الـ Admnistration overhead ، والـ Troubleshooting overhead ، والـ monitoring .

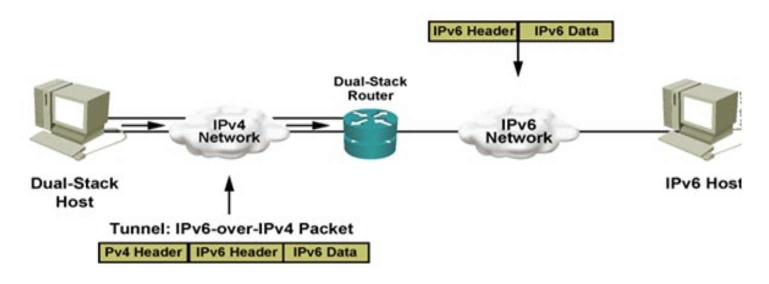
Tunneling : .2

يقوم الروتر بعمل Encapsulation لحزمة IPv6 داخل حزمة IPv4 . يقوم الجهاز الموجود عند نهاية شبكة الـ IPv4 بعمل Decapsulation لحزمة الـ IPv6 الأصلية ، ثم يعمل لها forwarding إلى وجهتها النهائية. يوضح الرسم أسفله هذه التقنية . للإشارة فالروترA وB يعملان بالـ Dual-satck .



Tunnel

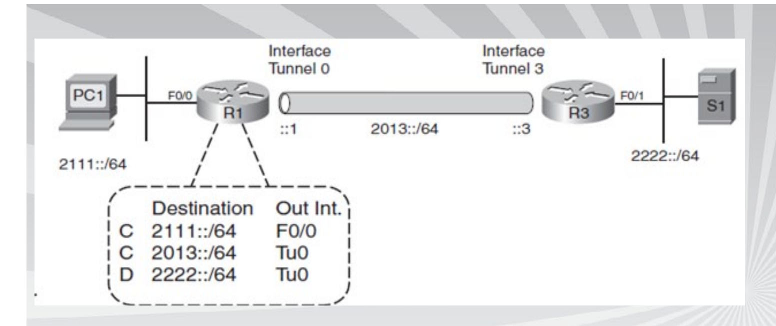
يمكن أيضاً استعمال الـ Tunnel بين host و روتر، كما هو موضّح في الشكل أدناه، حيث Dual stack hostمعزول , يستخدم الـ encapsulation tunnel للاتصال بالروتر الموجود عند حافة شبكة الـ IPv6 .



Isolated Dual-Stack Host Tunnel IPv6 Inside IPv4

Point-to-Point IPv6 Tunnels :

بعض الـ Tunnels تستخدم مفهوم الـ point-to-point ، في حين تستخدم أخرى مفهوم الـ multipoint. عند استعمال الـ point-to-point يمكن لجهازين(اثنين فقط) التواجد في نهايات الـ Tunnels. الـ point-to-point tunnels تعمل مثل الـ virtual point-to-point serial link . يوضح الرسم التالي هذا المفهوم، بالإضافة إلى بعض التفاصيل الأخرى.



	Destination	Out Int.
C	2111::/64	F0/0
C	2013::/64	Tu0
D	2222::/64	Tu0

مفهوم الـ IPv6 Point-to-Point Tunnel

لإنشاء الـ Tunnel كما هو مبيّن في الشكل ،فإنّ كل جهاز يتم إعداده بنوع من الـVirtual interface يسمى Tunnel interface . في هذا المثال، R1 يستخدم tunnel interface 0 و R3 يستخدم tunnel interface 3 . بالنسبة لأرقام الـ tunnel interface يمكن أن تكون أي عدد صحيح.

Point-to-Multipoint IPv6 Tunnels :

تسمح الـ Multipoint IPv6 Tunnels للروتر باستخدام tunnel interface واحدة لإرسال الـ Packets إلى العديد من الـ remote routers . و يمكن القول بأنّها تعمل كالـ LAN أو شبكة الـ Non-Broadcast Multi-Access (NBMA) كالـ Frame Relay .

Tunneling تمنح المهندسين إمكانية تجنب الإعداد الكامل للـ IPv6 على جميع الأجهزة. ولكن ، فإنّ جميع طرق الـ Tunneling تضيف المزيد من الـ Overhead على الروتر الذي يقوم بعملية الـ Encapsulation و الـ Decapsulation . لهذا يجب على المهندس التفكير ملياً في الفوائد المترتبة على الإعداد الكامل للـ IPv6 على جميع الأجهزة مقابل استخدام الـ Tunnels .

للـ Tunnels أيضاً العديد من الايجابيات والسلبيات. عموماً، الـ point-to-point tunnels تعمل بشكل أفضل عندما يرسل ترافيك الـ IPv6 بشكل منتظم و دائم . أما فيما يخص الـ multipoint tunnels تعمل عادة أفضل عندما يحدث حركة مرور ترافيك الـ IPv6 بين الفينة والأخرى ،يعني في الحالات التي يكون فيها حجم ترافيك الـ IPv6 قليل .

للـ multipoint tunnels قدرات ديناميكية متعددة تسمح للـ Hosts بتشكيل dynamic tunnelsمع الروتر دون الحاجة إلى إضافة أي إعدادات إضافية على الروتر.

Generic Routing Encapsulation (GRE) .1.2 و tunnels : Manually configured tunnels (MCT)

الـ MCT و الـ GRE توجد لديهما أوجه تشابه كثيرة، بما في ذلك إعدادهما على الروتر، كلاهما يحددvirtual

بين point-to-point link 2 routers IPv4 لأجل عمل forward لحزم الـ IPv6 IGP routing protocols . IPv6 تعمل من خلال هذا الـ virtual links لدعم الـ IGPs بالإضافة إلى ميزات أخرى . الـ routers سيحددون link local addresses على هذه Links، وسيسمحون بعمل forwarding لترافيك الـ IPv6 multicast. و كِلا النوعين يسمحان بإعداد بعض الميّزات الأمنية الإضافية على الـ Tunnel interfaces. وأخيراً , هما معاً يتطلبان static configuration لـ كِلا tunnel source و destination IPv4 addresses. tunnel

هذه الـ tunnels تعمل مثل الـ IPv6 native ، يشغلان الـ IPv6 IGPs باستخدام link local address، ولا تتطلب أي static route . و يكاد ألّا يوجد أي فرق عملي بين التقنيتين، و يلخص الجدول التالي الميزات الرئيسية لكل تقنية، مع إبراز بعض الفروق الصغيرة.

GRE	Manual Tunnel	
2784	4213	RFC
tunnel mode gre ip	tunnel mode ipv6ip	Tunnel mode command
1476	1480	Passenger MTU default
نعم	نعم	دعم الـ IPv6 IGPs ؟
نعم	نعم	Forwards IPv6 multicasts?
نعم	نعم	يستخدم static configuration للـ tunnel destination ؟
نعم	لا	يدعم العديد من الـ passenger protocols؟
IPv6 EUI-64 باستخدام lowest numbered interface's MAC address	FE80::/96 زائد 32 bits من tunnel source IPv4 address	الـ link local address مبنية على

2.2. ISATAP Tunnels و: Automatic 6to4 Tunnels

الـ multipoint tunnel لا تحدد explicitly للـ tunnel endpoint IPv4 addresses. بدلاً من ذلك، الـ destination IPv6 address لحزمة الـ IPv6 القادمة تحدد الـ IPv4 address التي سيستعملها الروتر لعمل encapsulating و forwarding للحزمة. لأن الـ tunnels تعتمد على الـ IPv6 address لتحديد الـ destination IPv4 address لهذه الـ tunnels، لهذا يجب على مهندسي الشبكة إنفاق المزيد من الوقت في البداية للتخطيط للـ IPv6 و الـ IPv4 addresse المستعملة.

يمكنك استخدام الـ ISATAP–the Intra-site Automatic Tunnel Addressing Protocol لتحديد الـ IPv4 address لـ remote site لأجل عمل tunneling لحزم الـ IPv6 . نتيجة لذلك ، يمكنك إنشاء dynamic multipoint tunnel باستعمال الـ ISATAP بصفة عامة فإنّه يشبه الـ automatic 6to4 tunnels . الـ Multipoint IPv6 تعطي للمهندسين وسيلة جيدة لتنفيذ الـ IPv6 connectivity لفترات قصيرة من الزمن. تسمح هذه الـ tunnels إضافة new site بسهولة، مع إعداد أقل على أجهزة الروتر الموجودة، هذه الـ tunnels تدعم الـ tunneling مع الـ hosts . لكن لا تدعم الـ IPv6 IGPs . و يلخص الجدول أسفله الميزات الرئيسية لِكِلا التقنيتين مع بعض الفروق الصغيرة بينهما.

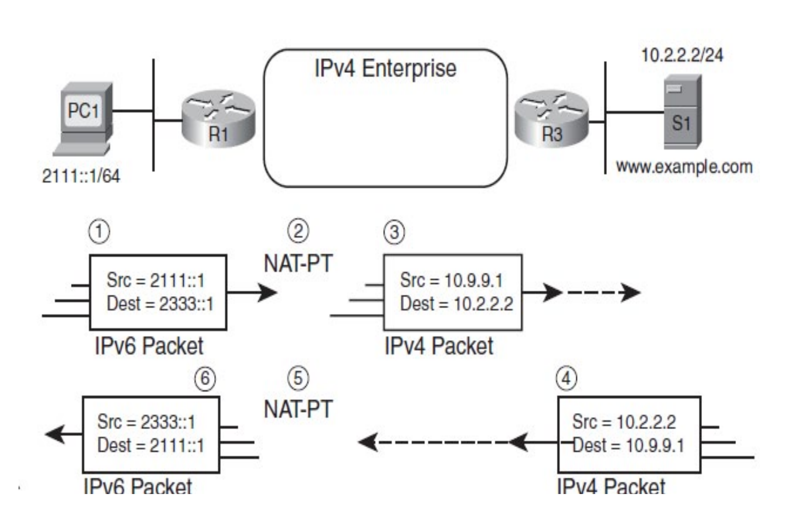
	Automatic 6to4	ISATAP
RFC	3056	4214
يستخدم IPv6 address prefix محجز	نعم (16/::2002)	لا
يدعم استخدام global unicast addresses	نعم	نعم
الـ Quartets المخزنة للـ IPv4 destination address	3/2	8/7
الـ End-user host addresses تتضمن الـ IPv4 destination	أحيانا	لا
الـ Tunnel endpoints IPv6 addresses تتضمن الـ IPv4 destination	أحيانا	نعم
يستخدم الـ EUI-6 لتكوين tunnel IPv6 addresses	لا	نعم

يسرد الجدول التالي تقنيات الـ Tuunels التي ناقشناها أثناء هذه الفقرة، جنباً إلى جنب مع بعض الملاحظات.

الطريقة	Static أوDynamic	Topology	المزايا وملاحظات أخرى
Manually configured	Static	Pt-pt	تعمل مثل virtual point-to-point link ، وتدعم الـ IGPs IPv٦ . تعمل جيدا للـ Tunnels التي تنقل ترافيك دائم. أقلOverhead قليلا من GRE .
GRE	Static	Pt-pt	Generic Routing Encapsulation نفس المزايا مثل الوسيلة السابقة، بالإضافة إلى أنّه يمكن أن يدعم بروتوكولات أخرى في الطبقة ٣ عبر نفس الـ Tunnel.
٦to٤	Dynamic	Mpt	يتطلب إعداد أقل بالمقارنة مع جميع الطرق الأخرى عند إضافة siteجديد. يدعم الـ Global Unicast ، مع بعض الإعدادات الإضافية. يستخدم الـ quartet الثاني والثالث لتخزين الـIPv٤ address .
ISARAP	Dynamic	Mpt	يدعم بسهولة الـ Global Unicast لجميع الـ Prefixes، يستخدم الـ quartet السابع والثامن لتخزين الـ IPv٤ address .

NAT Protocol Translation : .

هو أسلوب آخر من تقنيات الـ Transition ، ولكنّه ليس بديلاً عن الأساليب الأخرى السابقة التي تحدثنا عنها ، مثل الـDual stack و الـ Tunneling . بل يمكن استخدامه في الحالات التي يكون فيها التواصل مباشرة بين شبكات IPv6 فقط وIPv4 فقط. لن يكون استعمال الـ NAT-PT مناسباً في الحالات التي تتطلب الربط بين شبكتين لـ IPv6 ، لأنّنا سنحتاج لنقطتين للترجمة، و هذا لن يكون فعّالاً.
NAT-PT حصل على الجزء الأول من اسمه من خاصية الـ IPv4 Network Address Translation (NAT). الذي يقوم بترجمة عناوين الـIP address داخل الـ IP Header . في معظم الأحيان يتم تغيير الـ Private IP address إلى Public IP address لجعلها Internet routable . يترجم الـ NAT-PT كل من الـ source address و الـ destination address ، فهو يترجم بين عناوين الـ IPv4 و الـ IPv6 على حد سواء، لكنه يقوم أيضاً بترجمة الـ IPv4 header كاملاً إلى الـIPv6 header وبالعكس ، بالإضافة إلى Headers أخرى ، مثل UDP ، TCP وICMP . يتم إعداد وتنفيذ الترجمة علىNAT-PT روتر . الأجهزة الأخرى في الشبكة ليست على علم بوجود بروتوكول آخر، ولا بحدوث الترجمة.
ويبين الشكل أدناه مثالاً على حدوث عملية الـ Translation في الروترR1، حيث يقوم الـ PC1 الذي يستعمل الـ IPv6و الـ S1 الذي يستعمل الـ IPv4بتبادل الحزم.



حدوث عملية الـNAT-PT Translation في R1

1. (2111::1) PC1يرسل حزمة إلى 2333::1 ، R1يستقبل الحزمة.

R1.2 المُعَدّ مسبقاً بالـ NAT-PT، يستمع للحزم المرسلة إلى 2333::1 . R1 ثم يقوم بتحويل الـ IPv6 Header والـ Headers الأخرى إلىIPv4 standards .

3. يقومR1 بعمل forwardللحزمة إلى S1 .

4. S1يرسل حزمة إلىPC1، الـ Source address هي 10.2.2.2، الـ Destination addres هي 10.9.9.1 ، يقومR3 بعمل forward للحزمة إلى R1 .

5. R1 المُعد مسبقاً بالـNAT-PT، يستمع للحزم المرسلة إلى 10.9.9.1. R1 ثم يقوم بتحويل الـ IPv4 Header والـHeaders الأخرى إلىIPv6 standards .

6. . يقومR1 بعمل forwardللحزمة إلىPC1 .
لنجاح عملية التواصل في الشكل أعلاه، يجب على الـ NAT-PT أن يشارك أيضاً في تدفقات الـ DNS .



على سبيل المثال: قبل أن تتم عملية التواصل، سيرسل DNSv6 request الـPC1لمعرفة الـ IP address الخاصة بالـ www.example.com(S1) يجب على الروتر المُعد بـ NAT-PT في هذه الحالة بتحويل الـ requets بين Dns v4 وDns v6، ويجب الاحتفاظ بالـ address binding ليقوم الـ -NAT PT بالتحويل إلى الـ address الصحيحة.

وبهذا نكون قد ألقينا نظرة عامة على الأدوات المساعدة للانتقال بين IPv4 وIPv6. أتمنى أن أكون قد وفقت في الشرح وأضفت شيء للمحتوى العربي كما أتمنى أن ألقاكم في موضوع قريب إن شاء اللّه.حفظكم اللّه ورعاكم.

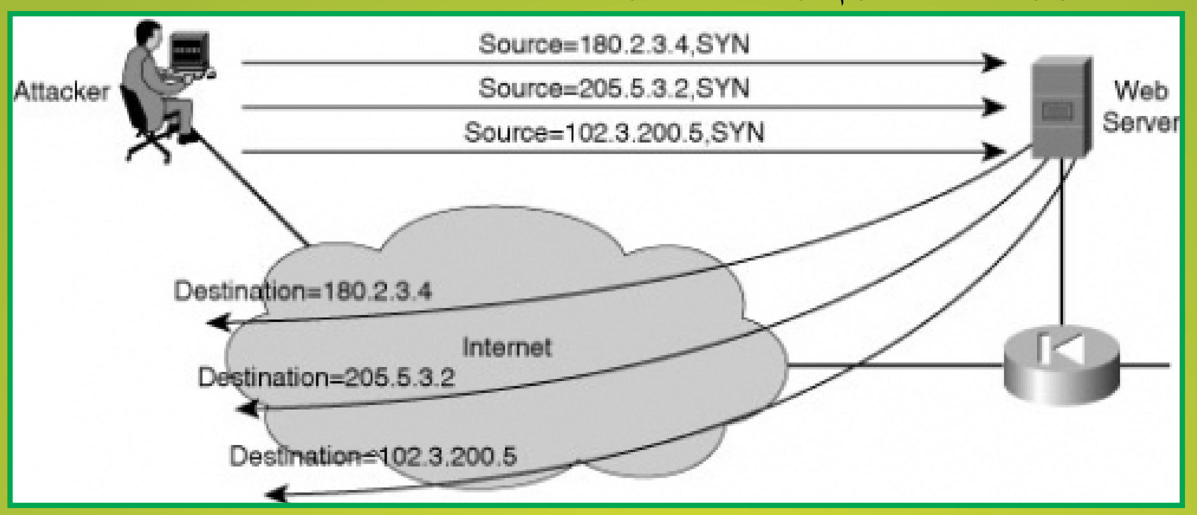


TCP-Intercept

من المشاكل التي تؤرق أي شخص مسؤول عن شبكة أو مجموعة من السيرفرات أو حتى موقع ما, هو استهداف الشبكة أو السيرفر المسؤول عنهم بهجمات من نوع DOS أو هجمات حجب الخدمة كما تسمى . أصبحت البرامج المتاحة لتنفيذ DOS ATTACK كثيرة جداً, وبإمكان أي شخص لا يفقه أي شيء أن يقوم بتنفيذ هجوم من هذا النوع فيسبب الكثير من المشاكل لسيرفر مهم أو حتى يسبب بطء ملحوظ في الشبكة ,لذلك فمن المهم أن تتأكد من أنّ الشبكة لديك محصـّنة ضد هذه الهجمات . خلال هذا المقال سأتحدث بإذن اللّه عن خاصيـّة موجودة على روترات Cisco تمكنك من رصد ومنع هجمات الـ DOS التي تعتمد على رسائل الـ SYN و تسمى SYN Flooding .

شرح SYN Flooding Attack

هذه الهجمة تستغل قصور موجود في بروتوكول الـ TCP ، كما نعرف فأي اتصال يعتمد على TCP يبدأ بما يعرف بـ three-way handshake و جميعنا مر بهذه العملية أثناء دراسة CCNA , فكرة هذا الهجوم تعتمد على قيام الهكر من خلال الاتصال بإرسال رسالة SYN إلى السيرفر, و بالطبع يقوم السيرفر بالرد عن طريق إرسال رسالة من نوع SYN/ACK و ينتظر الـ ACK الأخيرة من الطرف الأخر , لكن الهكر هنا بدل من أن يتم الاتصال ويرسل ACK يقوم بإرسال SYN مرة أخرى وكأنـّه ينشىء اتصال جديد ,الفكرة هنا أنـّه يقوم بإرسال فيض من رسائل الـ SYN ولكن بعناوين IP مزوّرة فيعتقد السيرفر أنـّها من مصادر مختلفة,وبهذا يغرق السيرفر بهذه الاتصالات شبه المفتوحة Half-Open Connection و أحياناً تسمى Embryonic Connection ، وهكذا حتى يصل السيرفر إلى وضع لا يستطيع معه استقبال أي SYN أخرى حتى ولو من مستخدم مسالم يحتاج إلى استخدام السيرفر ، بهذه الطريقة تم حجب الخدمة عن الجميع . هذه الصورة توضح الفكرة العامة للهجوم .

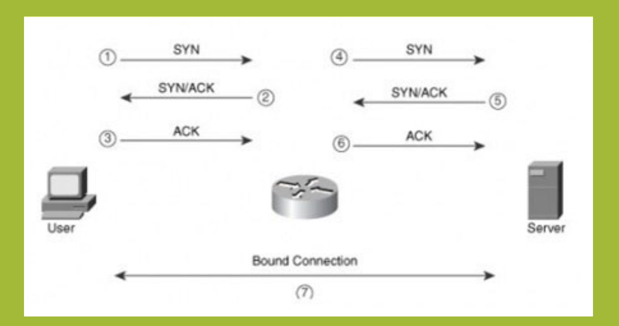


شرح خاصية TCP Intercept

طرق التصدي _و هي الهدف الأساسي للمقال_ لهذه الهجمة كثيرة ولكنـّي سأتحدث عن الطريقة التي تتبعها Cisco في الحماية ويمكنك تنفيذها على معظم الروترات . لهذه الخاصيـّة وضعين : الوضع الأول يسمى Watch Mode, و الثاني يسمى Intercept Mode, و في الجزء التالي سنعرف فكرة كل من الوضعين .

Intercept Mode

في هذا الوضع يكون للروتر دور إيجابي في المشاركة للتصدي لهذا الهجوم . أنظر إلى هذه الصورة أولاً لتعرف ماذا أقصد .



لاحظ معي ترتيب عملية الـ three-way handshake عندما يبدأ المستخدم الاتصال بالسيرفر :

1. يرسل المستخدم SYN إلى السيرفر.
2. عندما تصل الـ SYN إلى الروتر لا يقوم بإرسالها إلى السيرفر بل يتحمل عناء الرد و إرسال SYN/ACK إلى المستخدم .
3. فيقوم المستخدم بالرد و إرسال ACK لإتمام الاتصال , المفترض أنّ المستخدم يظن بأنّه يتصل بالسيرفر وليس بالروتر كما يحدث .
4. بعد أن تأكد الروتر من أن العملية سليمة ومكتملة يبدأ بإخبار السيرفر بهذا الاتصال فيرسل له SYN .
5. يرد السيرفر بـ SYN/ACK .
6. يرسل الروتر ACK لإتمام الاتصال .

بهذه الطريقة يعلب الروتر دور الوسيط P roxy بين المستخدمين و السيرفر , فبمجرد أن يرى الروتر أي عملية بدء للاتصال من قِبَل المستخدم , يقوم على الفور بالتعامل معه وعدم إرسال هذا الاتصال إلى السيرفر بعد أن يتأكد من اكتماله , وأنّه ليس جزء من هجوم SYN-Flood . الجدير بالذكر أنّ هذه العملية شفافة تماماً بالنسبة للطرفين السيرفر و المستخدم , فلن يشعر أي منهما بأي تغيير , وإذا قام الهكر بتنفيذ الهجوم السابق فعندها سيشعر الروتر بشيء غير طبيعي من كمية الـ Half-Open Connection التي لا تكتمل , فعندها يقوم الروتر بإرسال RST بعد Timeout معيّن يتأكد بأنّه الـ Connection المطلوب, عندها تكتمل . وبعد إرسال RST إلى مصدر هذا الاتصال يقوم الروتر فوراً بإزالته من على الـ Buffer, وهذا كله دون أن يشعر السيرفر بأي شيء .

Watch Mode

هذا هو الوضع الآخر الذي قد تُفضل استخدامه بدلاً من Intercept Mode , أولاً , لماذا قامت سيسكو بتطوير الخاصيّة لتشمل وضع آخر وهو Watch Mode ؟ بالطبع لحل مشكلة و إضافة ميزة لم تكن في الـ Intercept mode , مشكلة الـ Intercept mode أنّه في معظم الوقت لا يواجه السيرفر أي SYN Floods, ففي هذا الوقت يتحمل الروتر عناء كبير في عمل three-way handshake مرتين, الأولى هي المستخدمة وبعد أن ينتهي يقوم بتكرارها مع السيرفر , فتخيل تضاعف عدد المفاوضات الخاصة بـ three-way handshake, فهذا سيضع حمل كبير على البروسيسور , لهذا فالـ Watch Mode سيعمل بطريقة مختلفة لتقليل الحمل على البروسيسور , فدوره أغلب الوقت سيكون سلبي مقارنة بالـ Intercept Mode , فيقتصر عمله معظم الوقت على المراقبة فقط لأي اتصال TCP يمر من خلاله ولن يكون طرف نهائياً في أي اتصال كما حدث مع الـ Intercept mode , فإذا لاحظ أنّ الاتصال استمر لوقت معيّن (يمكن إعداد هذا الوقت حسب الحاجة) ولم تكتمل الـ three-way handshake بعد , فيقوم بفصل الاتصال فوراً عن طريق إرسال RST , وبهذا فأي half-open Connection على السيرفر سيقوم الروتر بالتعرف عليه وإزالته و تفشل أي محاولة لتنفيذ SYN Floods على السيرفر .

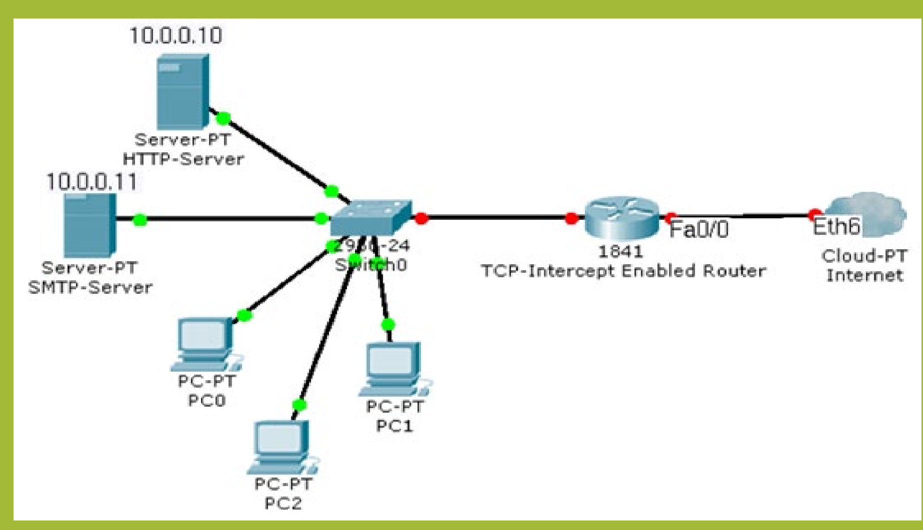
إعداد خاصية TCP Intercept

في الحقيقة إنّ طريقة الإعداد و تفعيل هذه الخاصية سهل جداً , بل صدق أو لا تصدق فلكي تقوم بتفعيل هذه الخاصية ستحتاج إلى أمر واحد فقط , لكن سيبقى هناك المزيد من الإجراءات و الأوامر المهمة التي ستستخدمها بعد ذلك لكي تعمل الخاصية بالشّكل الأنسب و الأفضل بالنسبة لشبكتك, فتعالوا نبدأ ونتعرف على أبعاد هذه الأوامر .

- **الخطوة الأولى : تفعيل خاصيّة TCP Intercept - إجباري**

Router(config)# ip tcp intercept list extended_ACL

هذا الأمر يقوم بشيئين مهمين جداً ,قبل أي شيء يقوم بتفعيل الخاصيّة وبعد ذلك يقوم بتحديد البيانات_TCP Sessions_ التي سيتم مراقبتها عن طريق تلك الخاصيّة , بالطبع لا نحتاج إلى تفعيل هذه الخاصيّة بالنسبة لأي اتصال TCP يمر من خلال الروتر , فالهدف الرئيسي من هذه الخاصيّة هو الحماية من هجمات SYN Flooding الموجّهة إلى السيرفرات , فلماذا يتم تفعيل الخاصية على أي اتصال TCP يتم بين جهازين عاديين !؟, ولتحديد الاتصالات التي سيتم تفعيل الخاصيّة لها, ستكون البيانات الموجّهة إلى أي سيرفر لديك تريد حمايته من فيض الهجمات للتقليل من الضغط على الروتر , فمثلاً في هذه الشبكة



لدينا سيرفران نحتاجهما لتفعيل الخاصيّة لهما فقط ,لكي نقلل الحمل من على الروتر وأيضاً لأنّ هذه الهجمات لن توجّه إلى أي Host عادي , سنقوم أولاً بإنشاء Access-list, نحدد بها الترافيك الذي سيتم مراقبته عن طريق هذه الخاصيّة, وهنا يجب أن أقول أنّك مجبر على استخدام Exteneded Access-List في هذه الحالة

```
Router(config)# access-list 100 tcp permit tcp any host 10.0.0.10 eq 80
Router(config)# access-list 100 tcp permit tcp any host 10.0.0.11 eq 25
Router(config)# ip tcp intercept list 100
```

الأوامر السابقة قامت بعمل الآتي , أولاً إنشاء Access-list نحدد بها الترافيك التي نريد أن تتم مراقبتها ,و هي بالطبع كل ما هو موجه إلى أي من السيرفرين بغض النظر عن الـ source لأنّه مجهول , وهنا استخدمنا الـ access-list استخدام غيّر عملها الأساسي و هو السماح أو منع مرور شيء معيّن, بل كانت مجرد أداة تقوم بعمل Match لبعض الترافيك , بعد أن قمنا بإنشاء الـ access-list, استخدمنا الأمر ip tcp intercept بمرجعية لـ access-list السابقة , كان من الممكن أن تكون الأوامر بهذا الشكل

```
Router(config)# access-list 100 tcp permit tcp any any
Router(config)# ip tcp intercept list 100
```

ولكن بهذه الطريقة الغبية سيقوم الروتر بمراقبة أي اتصال TCP يمر من خلاله , و سيكون عبارة عن بروكسي بمعنى الكلمة بين الجهتين, و لا أعتقد بأنّه سيكون لديه موارد كافية يوفرها لباقي العمليات بسبب هذه الطريقة , بهذا تكون قد قمت بتشغيل الخاصيّة و أي أمر آخر يأتي بعد ذلك أو اختياري فما سبق فقط هو الضروري لتشغيل الخاصيّة .

• الخطوة الثانية : تحديد الـ Mode - اختياري

```
Router(config)# ip tcp intercept mode {intercept | watch
```

هنا نقوم بتحديد الـ Mode الذي نريده , والـ Default Mode هنا هو Intercept , فإذا وجدت أنّ CPU يعاني من هذه الخاصيّة فبإمكانك تحويله إلى Watch Mode .

• الخطوة الثالثة : تعديل الـ Timers - اختياري

```
Router(config)# ip tcp intercept watch-timeout seconds
Router(config)# ip tcp intercept finrst-timeout second
Router(config)# ip tcp intercept connection-timeout seconds
```

لدينا هنا ثلاثة عدادات رئيسية , الأمر الأول يقوم بتحديد عدد الثواني التي سينتظرها الروتر في حالة الـ Watch Mode لكي تنتهي إجراءات الاتصال 3WAY-Handshake بين طرفي الاتصال , فمثلاً : قام شخص من الانترنت ببدء اتصال مع أحد سيرفراتنا المحميّة بهذه الخاصيّة, وبدأ بإرسال SYN, ورد عليه السيرفر بـ SYN\ACK, ولاحظَ أنّ الروتر هنا يعمل في وضع WATCH لأنّه لم يتدخل, فقط اكتفى بالمراقبة , الآن عدد الثواني التي سينتظرها الروتر لكي يكتمل الاتصال و يتم إرسال ACK إلى السيرفر قبل أن يعتبر الروتر أن هذا الاتصال خبيث, و يقوم بفسخه عن طريق إرسال RST إلى السيرفر ثم يقوم بتحديد هذه المدة عن طريق هذا الأمر . الـ Default لهذا الأمر هو 30 ثانية .
و الأمر الثاني أقل أهمية ونادراً ما يتم تعديله, وهو لتعديل المؤقّت الذي يحدد الوقت الذي سينتظره الروتر عندما يرى أي من طرفي الاتصال قام بإرسال FIN or RST , والمعلوم أنّ الروتر ينتظر 5 ثواني قبل أن يقوم بمسح معلومات الاتصال من الجدول الخاص به و يُهمله لأنّه انتهى .
والأمر الثالث يحدد المدة القصوى لأي اتصال TCP تم إكماله و تبادل الـ 3Way-Handshake ,ولكنّه أصبح IDLE ولا تمر أي بيانات به . والـ Default لهذا الأمر هو 24 ساعة قبل أن يتم قطع الاتصال .

• الخطوة الرابعة : تعديل قيم الـ Thresholds - اختياري

هذه القيم مهمة جداً, لأنّ الروتر يعتمد عليها ليعرف هل هناك Flooding Attack أم لا , تعالوا نرى أول أمرين لنفهم أكثر

```
Router(config)# ip tcp intercept max-incomplete high number
Router(config)# ip tcp intercept max-incomplete low number
```

ما تحدده هذه الأوامر هو متى يبدأ الروتر في عملية مسح للـ half-open connection , فإذا بدأ الهكر في عملية فتح أكثر من TCP session ليطبّق SYN Flooding على أحد السيرفرات , فعندما تصل هذه الـ half-open connection إلى الرقم المحدد في الأمر الأول_high_ فعندها يشعر الروتر أن هناك شيء غير طبيعي لأنّ عدد الاتصالات الغير مكتملة وصلت إلى هذا الحد ,فالأمر الأول أشبه بِتنبيه للروتر عن ارتفاع في عدد هذه الاتصالات الخبيثة , عندها ماذا يفعل الروتر ؟ يقوم فوراً ببدء عملية مسح لهذه incomplete connection حتى يصل إلى قيمته الصغرى التي يتم تحديدها في الأمر الثاني , وهذا مثال للتوضيح :
إذا تم إعداد القيم بهذا الشكل

```
Router(config)# ip tcp intercept max-incomplete high 1000
Router(config)# ip tcp intercept max-incomplete low 500
```

و أنا سأتقمّص دور الهكر المؤذي و أحاول تطبيق هجوم SYN Flood على أحد السيرفرات, وبدأت بإرسال SYN متتابعة إلى السيرفر المستهدف لعمل half-open connection , ولأنّ الشبكة مؤمّنة فلاحظ معي ما سيحدث , عندما يصل عدد الـ half-open connection إلى 1000 عندها يشعر الروتر أن المرحلة (threshold)تم تجاوزها ويبدأ بعملية مسح لهذه الـ connection حتى تكون أقل من الـ low threshold , بمعنى آخر سيقوم بمسح الـ incomplete connection حتى تكون أقل من الـ low threshold ,أي سيكون عدد الـ half-open connection حوالي 499 أي أقل من القيمة الصغرى التي حددناها , وبهذا كل ما تصل half-open connection إلى 1000 يتم فوراً تقليلها إلى 499 وهكذا يفشل الهكر التعس في تنفيذ الهجوم . الـ Default لهذه القيم هو 1100 كحد أقصى و 900 كحد أدنى .

```
Router(config)# ip tcp intercept one-minute high number
Router(config)# ip tcp intercept one-minute low number
```

أمرين آخرين لن يصعب فهمهما إذا فهمت الجزء السابق , عندما كنّا نقوم بإعداد الـ threshold في الجزء السابق, لابد من أنّك لاحظت كلمة max-incomplete, والتي تم استبدالها بـ one-minute , ففي الحالة الأولى _max-incomplete_ المقصود هنا هو إجمالي عدد الـ half-open connection أي الـ total , أما في حالة one-minute, فأنت بهذا تحدد قيم الـ threshold بالنسبة لمدة معينة هي دقيقة , أي أنّه يقول هذا الأمر الآتي : إذا زاد عدد الـ half-open connection في -الدقيقة الأخيرة- عن كذا (high threshold) قم بتخفيض عددها إلى كذا (low threshold) , هذا هو الفرق الجوهري بين طريقتي الـ max-incomplete و one-minute , الأمر يبدو معقداً بعض الشيء , ولكن مع كثرة التطبيق ستجد الموضوع أبسط من مما تتوقع

- **الخطوة الأخيرة : تغيير الـ drop method - اختياري**

```
{Router(config)# ip tcp intercept drop-mode {oldest | random
```

عندما يتم تجاوز قيمة الـ high threshold , يبدأ الروتر في عملية إزالة لـ half-open connection كما قلنا سلفاً , هذا الأمر يحدد الطريقة التي يتّبعها الروتر في الإزالة , التصرف الطبيعي هو أن يبدأ الروتر بمسح الـ half-open connection الأقدم أولاً حتى يتم الوصول إلى الـ low threshold , يمكن تغيير هذه الطريقة باستخدام الأمر السابق لتكون عملية الإزالة لـ half-open connection بشكل عشوائي .

هكذا نكون قد انتهينا وأتمنى أن يكون هناك من استفاد وبالتوفيق .

شهادة شكر وتقدير

تتقدم إدارة موقع



First Arabic Magazine for Networks

أقدمها لكل المشاركين معنا في المسابقة الخاصة بالمحتوى العربي
لمساهمتهم ومشاركتهم في المسابقة وكونهم أكثر إيجابية من غيرهم

مؤسس ومدير موقع NetworkSet
المهندس أيمن النعيمي

2011 / 9 / 25

NetworkSet
First Arabic Magazine for Networks
المجلة العربية المتخصصة بالشبكات



Cloud Computing

Identification
رضوان اسخيطة
الجنسية : سورية
خريج تكنولوجيا المعلومات – مدرس اختصاصي للشهادات العالمية الاحترافية في الصيانة والشبكات – لدي مساهمات بتعريب ونشر المحتوى العلمي المعلوماتي
radozgo@gmail.com
SYRIA



حديثنا اليوم عن فكرة Cloud computing , وأساس الفكرة تقديم خدمات حوسبة للمستخدمين من خلال شبكة الانترنت , والحقيقة أنّ طبيعة عمل هذه التقنية هي سبب تسميتها بهذا الاسم , حيث أنّ هذه التقنية تتم من خلال حواسيب شبكية تنتشر كالسحاب في مختلف أرجاء العالم , وتوفّر هذه الخدمات للمستخدمين دون معرفتهم لحقيقة مكان تواجدها, بل تتم كافة عمليات المعالجة ضمن خوادم السحابة .

تعتمد السحابة الحاسوبية على فكرة وجود أكثر من مركز بيانات موزعة جغرافياً , وقد يصل توزيعها جغرافياً إلى أكثر من دولة , وهنا يمكن تطبيق تقنية الموارد الافتراضية (Virtualized resources) . والهدف الأساسي من السحابة الحاسوبية هو خدمة المستفيدين عند الطلب بغض النظر عن موقع مركز البيانات .

من أهم فوائد هذه التقنية هو أنّها توفر المميزات الآتية :

1 -التوفير: فبدلاً من أن يشتري المستخدم أدوات وبرامج يحتاج إليها في عمله, تقوم هذه الشركات بتوفير المتطلبات اللازمة مقابل الاستخدام فقط , والدفع يكون مقابل الاستخدام .

2 -إمكانية الدخول على موقع الشركة واستخدامه من أي مكان في العالم وعبر أكثر من جهاز, وكل ما يحتاج إليه هو اتصال بالإنترنت فقط، كذلك يستطيع المستخدم الاستفادة من المواصفات الجيدة للخوادم التي يعمل من خلالها على ملفاته، لأنّه لا يستطيع على المستوى الشخصي توفير أجهزة وخوادم ذات مواصفات عالية.

3 -تقوم بتوزيع وحمل توفير الخدمات الإلكترونية للمستفيدين عند الطلب على أكثر من مركز بيانات.

4 -توفر مرونة في موضوع زيادة السعة الاستيعابية لمركز البيانات.

5 -تؤمن سرعة توفير الخدمات للمستفيدين عند الطلب في حالة حدوث كوارث.

6 -توفر الخدمات الالكترونية للمستفيدين على مدار الساعة.

7 -مرونة نقل البيانات بين مراكز البيانات دون التأثير على الخدمة المقدمة للمستفيدين.

8 - الاستفادة القصوى من جميع مراكز البيانات افتراضياً.

وعلى النقيض فإنّ العديد من الشركات العالمية قد أبدت تحفظها على الانتقال لهذه التقنية بسبب عدم الجاهزية التقنية لما تتطلبه هذه التقنية من تجهيزات وتقنيات ذات مستوى عالي .

وكذلك في عامل الأمن من أهم العوائق أمام انتشار هذه التقنية , ولهذا فإنّه يوصى بتطبيق بعض المحاذير عند استخدام هذه التقنية ومنها :

1 -استخدام SAML (Security Assertion Markup Language): وهي لغة تأكيد توصيف النص التي تسمح للمستخدم بتسجيل الدخول مرة واحدة لمواقع ويب التابعة لها ولكن بصورة منفصلة .وقد تم تصميم هذه اللغة لقطاع الأعمال, خصوصاً بين الشركات والمستهلكين .

2 -استخدام برتوكول OpenId: وهو بروتوكول يدعم عدة مواقع ولا يدعم موقع واحد, وببساطة فإنّ عمله يقوم على أنك لاتحتاج للتسجيل في الموقع إلاّ مرة واحدة, وسيتم التعرف عليك تلقائياً دون الحاجة للتسجيل مرة أخرى لكي تتم معالجة التحقق والمصداقية.

3 -من المهم أن تستخدم الشركات المزودة TriCipher's SAML, وهي بنية تحتية لمصادقة الدخول, وتقوم بحماية المواقع والمنافذ لأي شركة على الشبكة العنكبوتية .أيضاً يعطي دخول آمن للمستخدمين ويصل إلى 250 مشترك .

البرمجيات والحلول المبتكرة وفقاً لهذه التقنية

حلول التخزين

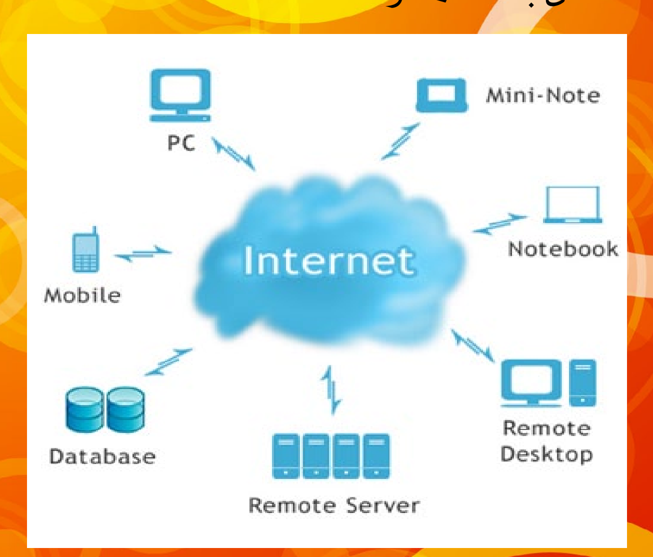
حلول التخزين السحابي في مجال حماية البيانات، يمنح المؤسسات مرونة وخيارات غير مسبوقة عند إستبدال وحدات التخزين الشريطية بحل سريع وآمن ومنخفض التكلفة يتيح لها ترحيل البيانات إلى بيئات التخزين السحابية بسهولة.

ومن هذه الحلول المضافة إلى منظومة "وايت ووتر" كل من حلول "ويندوز ازور" (Windows Azure)للتخزين السحابي؛ وحلول "راكسبيس كلاود فايلز" وهذه الحلول تقدم خدمات لإدارة عمليات استرجاع وتخزين البيانات .

حلول البريد الإلكتروني

وهي الحلول الملائمة جداً للشركات التي تستعمل خدمة البريد الإلكتروني مع عدد ضخم من الموظفين, وجاء التطبيق الأمثل لهذه التقنية مع عملاق برامج البريد الإلكتروني مايكروسوفت حيث طورت نظام اسمه Microsoft exchange online Service

حيث يعتبر هذا النظام حلاً ممتازاً للشركات المتوسطة الحجم, حيث يمكنها أن تخزن بريدها الإلكتروني الكامل لكل موظفيها والوصول إليه من خلال هذا النظام دون تكبد عناء شراء نسخ ويندوز ونسخ برنامج Exchange المكلف لكل موظفيها, بل على العكس تتكفل مايكروسوفت بكافة الإعدادات وضمان الاستمرارية والأمان الخاص بتلك المعلومات .



هل السحابة الحوسبية هي حل حتى للمستخدم المنزلي ؟

بالنسبة لي نعم , بالرغم من أن متطلبات المستخدم المنزلي محدودة, إلّا أنّ الكثير من الشركات ومزودات خدمة الإنترنت يقدمون هذه الخدمة للمشتركين, وهذه الخدمة تتنوع استخداماتها المنزلية مابين التخزين والنسخ الاحتياطي أو خدمة استخدام التطبيقات دون الحاجة لشرائها, وهذا ما أعتبره ميزة جبّارة للمستخدم المنزلي والمثال التالي يوضح ذلك :

لنفترض أنّ لدينا مجموعة صور أو نصوص ونحن بحاجة للتعديل عليها وتنسيقها قبل نشرها على موقعنا, ومادام هذا تقليدياً فإنّه يتطلب برامج مثل أدوبي فوتوشوب أو غيره, فإنّه مع وجود تقنية سحب الحوسبة فإنّه بإمكاننا القيام بذلك عبر متصفح الإنترنت ودون الحاجة لحيازة هذه التطبيقات المكلفة مسبقاً, وإنّ هذه التقنية تمنحنا إمكانية استخدام التطبيق دون الحاجة لتنصيبه على الجهاز, وكذلك إمكانية تخزين الملفات وإعادة تحميلها من أي مكان في العالم دون الحاجة إلى أن يكون لديك البرامج الداعمة لفتح هذه الملفات, و بالنسبة لي فإنّني بدأت بالتعرف على هذه التقنية من خلال اشتراكي مع مزود خدمة الإنترنت الألماني الذي أتاح لي خدمة سحابية مجانية, ويوفر مزود الخدمة خيارات لمشتركيه, حيث تتنوع أنواع المساحات السحبية التي يوفرها مابين مساحات تعمل كمخدم ألعاب ومساحات تعمل كمخدم تطبيقات ومساحات تعمل كمخزن للبيانات, كما يقدم خيارات تتعلق بالمساحات المطلوبة وعدد المعالجات المسؤولة عن هذه المساحة .



ومن المتوقع ان تستعمل هذه التقنية بشكل عام خلال الفترة المقبلة كبديل لكافة خيارات التخزين المحلي والنسخ الاحتياطي لما لها من توفير في تكاليف التخزين والحماية والإدارة .

رحلة في أعماق روتر

[الحلقة الأولى]



بداية هذه المقالة تعتبر متقدمة وعميقة نوعاً ما, حيث أنّها تتحدث عن مكونات وأجزاء الروتر ودور كل مكوّن أو جزء أو قطعة بداخله بشيء من التفصيل، لكن ليس معنى هذا أنّ هذه المقالة للمتقدمين فقط, إنّما هي للجميع, بل و تساعد المبتدئين لفهم الكثير من الغموض في كيفية تنفيذ الروتر لمهامه، كما أنّها ستساعد الكثيرين في فهم الكثير من المواضيع المتقدمة مثل تقنية الـ CEF الخاصة بشركة سيسكو. والآن هيا بنا نبدأ,ولكن قبل البدء أود التنبيه إلى من ليس لديه عدة الغوص بأن يرجع, فإنّه سيكون عرضة للغرق، أقصد بذلك, أنّ تلك المقالة ليست للمبتدئين في المجال بشكل عام, ولكن أقصد بالمبتدئين هنا الحاصلين على الشهادة CCNA, أرجو أن يكون هذا واضحاً وإلّا فالبعض قد يكره المجال بسبب تلك المقالة وأنا غير مسؤول.



بدايةً إنّ دور الروتر هو توجيه البيانات بين المرسل والمستقبل, إذن يلزمنا قطع صلبة Hardware أو برمجية Software تقوم بالأدوار أو المهام التالية (وأريد منك أن تركّز معي جيداً لأنّنا سننطلق من هنا):

1 - في البداية يستلم الروتر الحزمة Packet من المرسل, أليس كذلك؟ إذن فهو يحتاج لقطعة صلبة أو برمجية تمكّنه من استلام واستقبال الحزمة Packet المرسلة إليه من على السلك.

2 - ثم يخزن تلك الحزمة Packet لكي يستطيع العمل عليها للوصول إلى غايته وهي تمريرها للوجهة المطلوبة, إذن فهو يحتاج لمكان ما أو قطعة صلبة أو برمجية يخزن فيها,وهي الذاكرة.

3 - ثم يبدأ العمل بالنظر في الرؤوس Headers المختلفة التي مع الحزمة Packet لمعرفة هل هي سليمة بفحصها Check, وأين الوجهة التي تريد الوصول إليها من خلال العنوان IP Address, وكذلك استبدال الرأس الخاص بالطبقة الثانية إلى العنوان MAC المخصص للقفزة التالية Next hop في رحلة الحزمة Packet، فهو إذن يحتاج لقطعة صلبة أو برمجية للقيام بكل ذلك.

4 - أخيراً إرسال تلك الحزمة Packet للمنفذ Interface التي ستخرج منه لوجهتها النهائية، إذن فهو يحتاج لقطعة صلبة أو برمجية عند منفذ الخروج outbound للقيام بذلك.

هذه المهام الأربع السابقة لابد من تنفيذها لكي يصل الروتر لهدفه وهو مساعدة تلك الحزمة Packet في الوصول لوجهتها النهائية, ولا تنسى أنّ من ينفذها ربما تكون قطعة صلبة أو برمجية. هذه هي النقطة الأولى التي أود أن نكون متفقين عليها...

ثانياً معظم الروترات تستخدم أحد هذه القطع الصلبة والأساسية لتوجيه الحزم Packets إلى وجهتها النهائية:

1 - Interface processors معالجات المنافذ.
2 - Central Processor Unit (CPU) المعالج.
3 - Memory الذاكرة.
4 - Backplane and switching fabric دائرة إلكترونية معزّزة.

والآن ما رأيك في أن نقوم بالربط بين المهام الأربع والقطع الصلبة في شرح نبين فيه وظيفة كل قطعة صلبة وما تقوم به من مهام، وأريد منك أن تلاحظ أنّه ربما القطعة الصلبة لا تقوم بالمهمة, ولكن القطعة الصلبة تقوم ببناء مكون برمجي Software هو الذي يقوم بتلك المهمة, أرجو أن يكون الكلام واضحاً, وإن لم يكن فحاول أن تقرأ تلك الأسطر أكثر من مرة.

مرة أخيرة نقول أنّ الروتر لكي يقوم بتوجيه الحزم يستخدم في ذلك أحد مكوناته أوقطعه الصلبة: دوائر إلكترونية أو رقائق معدنية أو ذاكرة أو معالج... الخ، أو يستخدم تلك القطعة الصلبة في بناء مكون برمجي ينوب عن القطعة في تنفيذ تلك المهمة.

ملحوظة هامة: سؤال/ مَنْ الأسرع في التنفيذ والأكفأ في الأداء, أن تقوم القطعة الصلبة بتنفيذ المهمة أم أن توكّل تنفيذها لمكون برمجي؟ (مثال للمكوّن البرمجي جدول التوجيه Routing Table) طبعاً القطعة الصلبة أسرع في التنفيذ وأكفأ, ومع ذلك قد نضطر في بعض الأحيان لاستخدام المكون البرمجي ولا نستطيع استخدام القطعة الصلبة لتنفيذ المهمة.

ملحوظة أخرى هامة: في بعض المهام يكون الروتر مُخيّر بين استخدام قطعة صلبة لتنفيذ المهمة أو مكوّن برمجي، وبمعنى أعلى وأدق أقصد بمُخيّر بأنّ هناك خيارات وطرق كثيرة لتوجيه الحزمة Packet, لذلك على المسؤول عن عمل الروتر اختيار الطريقة الأنسب لجهازه و شبكته.

والآن لنبدأ في شرح كل قطعة صلبة بشكل أكثر تفصيلاً...

أولاً: معالجات المنافذ Interface Processors

عند استقبال منفذ ما على الروتر لحزمة ما فإنّه يقوم بالتعامل معها من خلال معالج ذلك المنفذ، وتلك المعالجات مسؤولة عن المهام التالية:

1- فك رموز الإشارات الكهربية أو الضوئية عند وصولها عبر الوسائط المادية (حيث أنّ الحزمة تنتقل داخل وسط إمّا أن يكون كيبل نحاس أو كيبل فيبر وعلى شكل إشارة كهربية أو ضوئية).

2- ترجمة هذه الإشارات إلى أصفار وواحدات (0s and 1s).

3- نقل وتخزين الأصفار والوحدات إلى مكان ما بذاكرة الروتر.

4- تحديد البت الذي يشير إلى أنّ الحزمة قد انتهت، ويُعرف باقي المكونات والقطع بأنّه سيبدأ في استقبال حزمة جديدة.

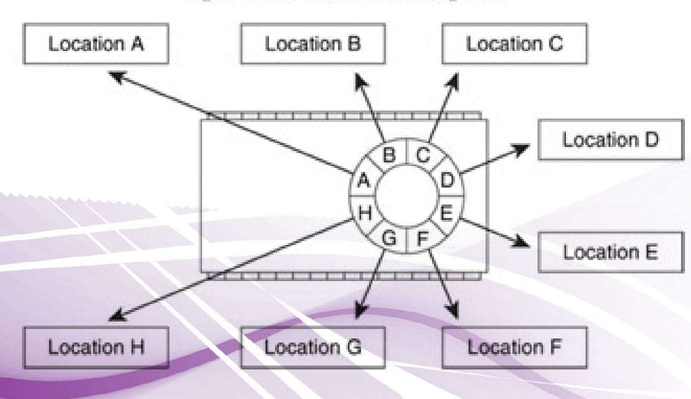
ولكن ما هي معالجات المنافذ؟ هي قطع صلبة, فهي عادة عبارة عن رقائق معدنيةChips , وهي متاحة تجارياً ومصممة خصيصاً لفك الإشارات وترجمتها إلى الحزم. وعلى سبيل المثال: إنّ أقدم وأشهرالرقائق استخداماً هي التي تستخدم في أجهزة الشبكات المحلية LAN (سويتشات شبكات الإيثرنت) لفك وترجمة الإشارات الكهربية إلى إطارات Frames.

تعرّفنا على عملية الترجمة من خلال الرقائق، ولكن كيف تتم عملية التخزين بالذاكرة؟ (لأنّنا ذكرنا أنّه يقوم بعمليتين أساسيتين هما الترجمة والتخزين)ومن هو المسؤول عن تحديد هذا المكان بالذاكرة؟ وما هي آلية استرجاع الحزمة وقت الحاجة من الذاكرة؟



معالجات المنافذ تقوم بنقل الحزم إلى الذاكرة عن طريق الوصول المباشر للذاكرة, بمعنى أنّها تنسخ الحزم وتحفظها في مكان ما بالذاكرة ويُحَدّد هذا المكان بناءاً على تعليمات العقل المدبر والمدير التنفيذي للروتر وهو نظام التشغيل IOS (سنناقش هذه النقطة في مقالات قادمة بإذن اللّه). حيث يتم تخزين مجموعة من العناوين تشير إلى الأماكن التي تم تخزين الحزم بها في الذاكرة, وذلك في ذاكرة مؤقته Buffer خاصة بالمنفذ وعلى شكل حلقي كما في الشكل التالي:

Figure 1-7. Interface Processor Ring Buffers



وللتوضيح أكثر, لاحظ أنّ كل مدخل في تلك الذاكرة المؤقته (التي على شكل حلقة) يشير إلى مكان مختلف في الذاكرة. فأوّل حزمة تصل يأخذ منها نسخة وتخزن في الذاكرة في مكان ما ويشار إلى هذا المكان في الموضع A كما هو موضح في الشكل السابق، في حين ستوضع الحزمة الثانية في الذاكرة في المكان المشار إليه في الموضع B، ثم الثالثة يشار إلى مكان تخزينها بالموضع C وهكذا...
أحب أن أؤكد على أنّ ما يُخزّن في الذاكرة المؤقتة الخاصة بالمنفذ هو عناوين تشير إلى أماكن التخزين الحقيقية بذاكرة الروتر وليس الحزم نفسها, فالحزم نفسها مخزنة بذاكرة ما بالروتر.
أخيراً عندما يقوم معالج المنفذ بنسخ الحزمة إلى مكان ما بالذاكرة ويصل إلى أن يشير إلى هذا المكان بالموضع الأخير في الحلقة H، ثم تأتي حزمة أخرى جديدة فإنّه يقوم باستخدام الموضع A في تكرار للعملية على شكل حلقة, لذا تسمى هذه الذاكرة المؤقتة بالـ transmit and receive rings حلقات الإستقبال والإرسال.
لاحظ أنّ هذه العملية تتم في كل منفذ على حدى وبشكل مستقل, فكل منفذ له ذاكرة مؤقتة buffer خاصة به أو قد تكون ذاكرة مشتركة بين المنافذ وهذا يعتمد على نوع وموديل الروتر, كما ويختلف حجم هذه الذاكرة حسب نوع المنفذ وإمكاناته.

ثانياً: المعالج CPU

يقوم المعالج بدور المحرك والمنفذ horsepower لأي عملية عامة تحتاج المكونات البرمجية لتنفيذها. ففي بعض موديلات الروترات يقوم المعالج بتنفيذ المهام الخاصة بتوجيه الحزم بأوامر من البرمجيات، بينما في موديلات أخرى يركز المعالج بالدرجة الأولى على عملية إدارة آلية عمل الروتر لتوجيه الحزم والتي تعرف بـ control-plane, بينما تصمم القطع الصلبة كالرقائق خصيصاً لتوجيه الحزم فيما يعرف بـ data-plane. ولاشك أنّ النوع الثاني أسرع وأكفأ لأنّ القطع الصلبة تنفذ مهامها بدون الاعتماد على المعالج, ويقوم المعالج فقط بإدارة عملية التوجيه للحزم.
ومن هذا يتضح سبب إجابتي السابقة على السؤال أيهما أكفأ وأسرع، حيث نلاحظ اعتماد المكونات البرمجية على المعالج لتنفيذ مهامها مما يشغل الروتر وقد يتوجب عليها انتظار دورها في عملية المعالجة, حيث أنّ المعالج لديه مهام أخرى بينما القطع الصلبة تقوم بتنفيذ مهامها بنفسها, لذلك سميت بـ Interface Processors.

ثالثاً: الذاكرة Memory

روترات سيسكو تستخدم الذاكرة لتخزين الآتي:
1 - الحزم أثناء عملية معالجتها.
2 - الحزم لحين يقرر الروتر إلى أين ستتم عملية التوجيه.
3 - جداول التوجيه والتحويل Routing and Switching tables.
4 - هياكل البيانات العامة general data structures (وهي التي ترجع إليها الرقائق Chips عند عملية تحويل الإشارات إلى حزم) وقانون التنفيذ executing code وغير ذلك...



بعض موديلات الروترات الخاصة بشركة سيسكو تحتوي على نوع واحد فقط من الذواكر مثل:
Dynamic random-access memory (DRAM) or synchronous dynamic random-access memory (SDRAM).
بينما هناك موديلات أخرى تحتوي على العديد من أنواع الذواكر ولأغراض مختلفة (ولعلنا نناقش هذه الجزئية في مقالات قادمة بإذن اللّه).

تبقيت جزئية هنا وهي المكون الرابع من القطع الصلبة Backplane and switching fabric دائرة إلكترونية معزّزة, وهذا سيكون موضوع الحلقة القادمة إن شاء اللّه تبارك وتعالى.
أعرف أنّي أطلت عليكم ولكن يشهد اللّه كم تعبت في استخراج هذه المعلومات وتبسيطها بقدر ما أستطيع لأهميتها في كثير من الموضوعات وخصوصاً المتقدمة, وأنا في انتظار استفساراتكم, شكر اللّه لكم حسن القراءة ولا تنسونا من صالح دعائكم.



تعريف بالمعيار ISO/IEC 27001:2005



جميع الشركات والمؤسسات والقطاعات الحكومية تمتلك معلومات مهمة وثمينة وقد تكون سرية للغاية, فهذه المعلومات تحتاج إلى منظومة أمنية تحميها من جميع المخاطر التي تهددها. فقد تختلف هذه المخاطر المحيطة بهذه المعلومات من سرقة إلى حذف أو تعديل للبيانات والمعلومات الموجودة بالمؤسسة.

ونظراً لوجود هذه المعلومات القيّمة بأكثر من مكان داخل أي مؤسسة ابتداءً من السيرفرات وسيرفرات النسخة الاحتياطية و Backup وانتهاءً بالمعلومات الموجودة على الحواسيب الشخصية للموظفين, فقد توجّب على الاختصاصيين إيجاد حلول أمنية مختلفة المستويات لمنع وصول الأيادي المشبوهة والولوج الغير مصرح له إلى هذه المعلومات, بالإضافة إلى ذلك العمل على رفع مستوى الإدراك لدى الموظفين وتدريبهم على أن يكونوا مسؤولين وحريصين على المعلومات التي بين أيديهم, وتدريبهم أيضاً على كيفية الاستجابة لأي طارئ أمني قد يحصل أثناء عملهم .



لذا ظهرت ضرورة أن يكون هناك معيار عالمي مختص بأمن المعلومات تستطيع أن تمتثل له جميع المؤسسات والمصارف وجميع قطاعات الأعمال والدولة, ويهدف للارتقاء بالواقع الأمني ويرسم الخطوط الأساسية للسياسات الأمنية المتّبعة, ويقوم بتنظيم عملية التوثيق المرتبطة بأمن المعلومات. وإيجاد الأدوات والحلول اللّازمة للوصول إلى المستوى المطلوب من أمن المعلومات, وذلك بالتوافق مع الثالوث الأمني المقدس (التوافرية, السلامة, السرية), وذلك للحيلولة دون التعقيدات التي قد تضر بالعمل وتؤذّر سير الأعمال .

فالتطور التكنولوجي المتسارع وتطور التهديدات المباشرة لها أدّى إلى تطور معايير أمن المعلومات. وتختلف هذه المعايير تبعاً للمخاطر التي قد يواجهها قطاع معيّن من الأعمال. فبالتأكيد المخاطر التي قد يتعرض لها بنك معيّن مختلفة نوعاً ما عن المخاطر التي قد تواجهه شركة عقارية , نظراً لاختلاف نوعية المعلومات وحساسيتها والعدد الكبير من الأشخاص المتعاملين معها بشكل أو بآخر, ولذلك تفرض سياسات أمنية مختلفة تماماً, وتكون أكثر تعقيداً وتكثيفاً في البنوك والقطاعات المالية والمصرفية عن غيرها من الأعمال .



هنالك معايير تمتاز بالشمولية والمطواعية مثل ISO/IEC 27701:2005الذي يُعتبر الأكثر انتشاراً والأكثر اعتماداً, فما هو الايزو 27001 ؟

في العام 1992 نشرت إدارة الصناعة والتجارة البريطانية (DTI) نظام إدارة ممارسة أمن المعلومات, وتحولت فيما بعد هذه التوصيات إلى معيار على يد المعهد البريطاني للمعايير القياسية في العام 1995 تحت اسم BS7799 , وتم تعديل هذا المعيار أكثر من مرة في عامي 1996 و1999, إلى أن اعتمدته المنظمة العالمية للمعايير القياسية تحت اسم ISO 17799 في العام 2000 . في العام 2005 وبعد عدة تطويرات وتعديلات اتخذَ هذا المعيار شكله واسمه الحالي ISO/IEC 27001مرفقاً بمجموعة من المعايير المُعرِّفة والمساندة لهذا المعيار ابتداء من ISO/IEC 27000 الذي يضع التعريفات الأساسية إلى ISO/IEC 27006 الذي يُعتبر دليلاً لعملية التسجيل والتصديق .

ISO/IEC 27001 يحدد المتطلبات اللّازمة لتجهيز وتشغيل ومراقبة ومعاينة وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات في سياق المخاطر للمؤسسات ككل. ويُنظّم المسؤوليات لجميع الأطراف المتعاملة مع هذه المعلومات, ويحدد أطر



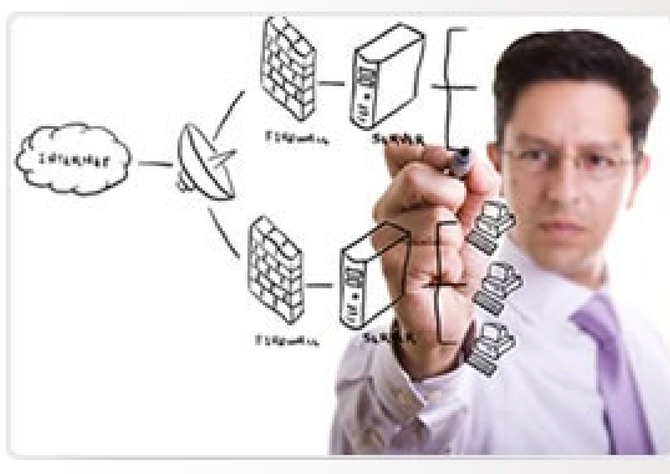
الاستجابة للمخاطر دون الخوض في تفاصيل كيفية الاستجابة , ومن خلاله تُحدد عملية توثيق تدابير سياسات الحماية والإجراءات وتعيين كل الخطوات اللّازمة لإدارة المنظومة الأمنية, ونشر الضوابط المتعلقة بها وربطها بتشريعات قانونية وتنظيمية ومراقبة الامتثال لهذه التشريعات من قبل الإدارة والموظفين. وقياس المستوى الأمني بشكل دوري, وتحديد نقاط الضعف التي يمكن أن تشكل تهديداً محتملاً إن كانت نقاط ضعف تشغيلية أو تقنية أو فيزيائية أو حتى بيئية, مثلاً (درجة الحرارة والرطوبة في غرفة السيرفرات) أو أي نقطة ضعف يمكن أن تسبب تهديداً محتملاً لاستمرارية عمل المؤسسة, وهذا التهديد يمكن أن يصبح خطر لابد من إنهائه أو التعامل معه أو ربما نقله (التأمين مثلاً).

و يجب أن يكون هنالك تقارير جاهزة بين يدي الاستشاريين الذين يقومون بتجهيز المؤسسة لتمتثل لمعيار الايزو, مثل تقرير تقييم نقاط الضعف (Vulnerability assessment report), و اختبار الاختراق (Penetration Test), وتقرير تحليل الفجوات الأمنية (Gap analysis report), و تقرير التدقيق الداخلي (internal audit report), وتقرير تقييم المخاطر (Risk Assessment Report), والعديد من التقارير الأخرى ليشكّلوا صورة واضحة عن الوضع الأمني الحالي للمؤسسة, وبعدها يتم على أساسه العمل على إنهاء نقاط الضعف والخلل وبناءً عليه يتم تفعيل/عدم تفعيل بعض الوظائف والعناصر المتعلقة بأجهزة أنظمة المعلومات (routers ,switches, mail servers, Web application servers ,firewalls/UTM , IDS ,IPS.......) , أو ربما ترقية (Update), أو ترقيع الفجوات الأمنية للأنظمة (System Patches الموجودة حالياً, وقد يتطلب الأمر بعض الأحيان استبدال بعض هذه الأنظمة .

وفي نفس الوقت الشروع بتأسيس سياسات وإجراءات أمنية واضحة تُعتمد من قبل إدارة المؤسسة للتعامل مع أي تهديدات قد تواجه المؤسسة وكيفية التصدي لهذه التهديدات. ووضع خطة دائمة لتطوير وصيانة هذه السياسات بشكل دوري وفقاً لحاجات المؤسسة, ووفقاً للتوسع الأفقي و العامودي في أعمالها .

ISO/IEC 27001 لا يفرض حلول معيّنة, ولا يأتي بالعصا السحرية التي قد تحوّل كل شيء آمن في لمحة بصر, بل يعطينا إرشادات, ويطرح علينا أسئلة محددة يجب أن (نعمل) على الإجابة عليها, وقد تكلف بعض الأسئلة آلاف الدولارات, وأشهُر من العمل .
فمثلاً : مؤسسة لديها Backup System فيأتي استشاري أو مدقق ISO/IEC 27001 ليطرح عدة تساؤلات :

1. في أي وقت و متى يتم أخذ نسخ احتياطية؟ وبناءً على ماذا؟
2. هل المعلومات مصنّفة لديكم؟
3. من لديه الحق بالوصول إلى هذه النسخ؟
4. كيف تخزن هذه النسخ وأين؟
5. ما مدى وثوقية وسائط التخزين؟ وما عمرها الافتراضي؟
6. هل النسخ الاحتياطية مشفرة أم لا ؟
7. هل النسخ الاحتياطية مؤشرة و مدلول عليها؟
8. أي نوع من المعلومات يتم نسخها ؟كلها أم جزء منها ؟
9. هل يتم النسخ الاحتياطي إلى مكان ما داخل المؤسسة أم إلى مكان آخر خارجها؟ ماذا لو حصلت كارثة ما؟ ,كالزلزال مثلاً .





كل هذه الأسئلة أو ربما أكثر بكثير يجب أن يجاب عليها من قبل المؤسسة, وهذا فقط على صعيد الـ Backup System (الذي هو جزء من إدارة استمرارية الأعمال), فما بالك بالباقي من المواضيع التي تتعلق بأمن المعلومات ؟ فهنالك اثنا عشر قسم لنظام إدارة أمن المعلومات (ISMS) :

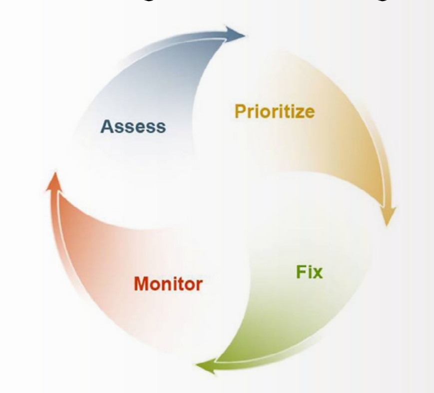
1. تقييم المخاطر Risk Assessment
2. السياسات الأمنية Security Policy
3. تنظيم أمن المعلومات Organization of Information Security
4. التحكم بالوصول Access control
5. إدارة الأصول Asset Management
6. أمن الموارد البشرية Human resource Security
7. الأمن الفيزيائي والبيئي (المتعلق ببيئة عمل الأنظمة) Physical and environmental Security
8. إدارة الاتصالات والتشغيل Communications and Operations Management
9. صيانة وتطوير واكتساب أنظمة المعلومات Information Systems Acquisition, development and maintenance
10. إدارة حوادث أمن المعلومات Information Security Incident Management
11. إدارة استمرارية الأعمال Business Continuity Management
12. الامتثال Compliance

تمر عملية الامتثال إلى ISO/IEC 27001 بثلاث مراحل أساسية :

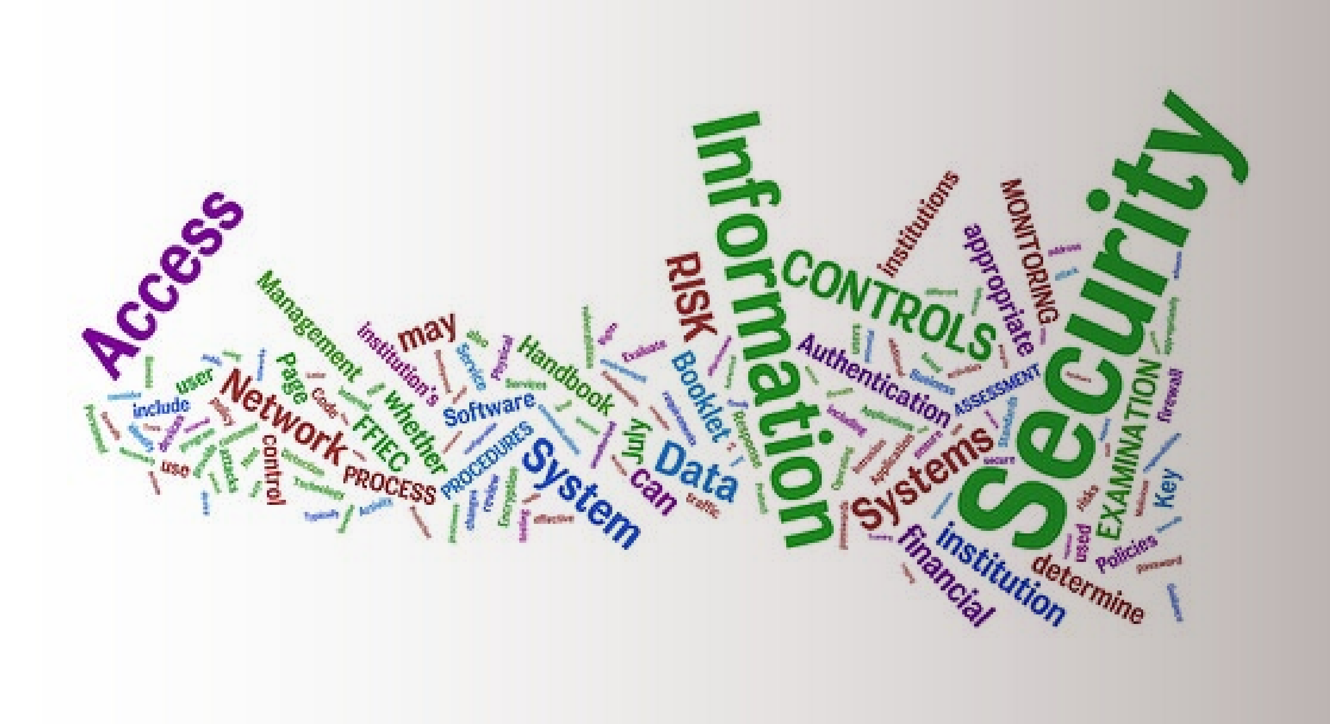
-**المرحلة الأولى** : استعراض غير رسمي لنظام أمن المعلومات ، على سبيل المثال: التحقق من وجود واكتمال الوثائق الأساسية ،مثل سياسة أمن المعلومات للمؤسسة, بيان التطابق (SOA), وخطة معالجة المخاطر (RTP), هذه المرحلة تعمل على تعريف المدققين الأمنيين مع المنظمة، والعكس بالعكس.

المرحلة الثانية: هي الامتثال و مراجعة التدقيق أكثر تفصيلاً و رسمية، والاختبار بشكل مستقل إزاء التدابير المتطلبة من قبل ISO/IEC 27001. وسوف يسعى المدققون للحصول على أدلة للتأكد من أنّه تم تصميم وتنفيذ نظام إدارة سليم, وفي واقع العملية (على سبيل المثال : يجب التأكد من أنّ اللجنة الأمنية أو أي هيئة إدارية مشابهة تلبي التدابير الناظمة والإشراف على نظام أمن المعلومات), لذا يجري عادةً تدقيق شهادة ISO/IEC 27001 من قبل المدققين المعتمدين من قبل المنظمة العالمية للمعايير القياسية.

- **المرحلة الثالثة** : تنطوي على متابعة استعراض أو مراجعة التدقيق للتأكد من أنّ المنظمة لا تزال تمتثل للمعيار. شهادة الصيانة الدورية تتطلب إعادة تقييم عمليات التدقيق الأمني للتأكد من أنّ نظام إدارة أمن المعلومات لا يزال يعمل على النحو المحدد والمقصود. وينبغي له أن يُحدَّث سنوياً على الأقل ولكن (بالاتفاق مع الإدارة), ولكنّه غالباً ما يجرى على نحو أكثر تواتراً، خصوصاً عندما يكون نظام إدارة أمن المعلومات لا يزال في مرحلة النضوج . لتكون المؤسسة مصدّقة وحاصلة على شهادة



ISO/IEC 27001 يجب أن تخضع لعملية التدقيق من قِبَل مدققين من خارج المؤسسة, وعادة ما يكونون من إحدى هذه الجهات TUV أو BSI المعتمدة من قبل المنظمة العالمية للمعايير القياسية (ISO), الذين يقومون بإصدار شهادة مدتها ثلاث سنوات, تضمن فيها بأنّ هذه المؤسسة تمتثل لتوصيات الايزو , وتقوم هذه الجهات بالتدقيق السنوي (مرة كل سنة) على كل ما يتعلق بنظام إدارة أمن المعلومات (ISMS).



بروتوكول العدد DHCP



نسمع كثيراً عن بروتوكول DHCP, و أغلبنا يقوم باستخدامه بشكل يومي, والكثير منّا يعرف لماذا نستخدم بروتوكول DHCP ولكن أردت في هذا العدد من مجلة Networkset أن ألقي الضوء على مبدأ عمل هذا البروتوكول الرائع, حيث أنّ DHCP هي اختصار لـ Dynamic Host Configuration Protocol, والذي يستخدم لتوزيع عناوين الـ IP وبعض الإعدادات الأخرى مثل الـ Subnet Mask و Default Gateway و DNS Server لأجهزة DHCP Clients المتصلة بالشبكة ، ويستخدم هذا البروتوكول بروتوكول UDP من خلال المنفذ 67 لإرسال الرسائل إلى DHCP Server والمنفذ 68 لإرسال الرسائل إلى DHCP Client .

فوائد استخدام بروتوكول DHCP :

يتم استخدام بروتوكول DHCP لتوزيع عنوانِ الـ IP وإعداداته بشكل أوتوماتيكي للأجهزة بدلاً من الحاجة لعمل هذه الإعدادات بشكل يدوي على كل من أجهزة DHCP Clients ، وبالتالي فإنّ استخدام بروتوكول DHCP يوفر الوقت والجهد ، كما أنّ احتمال حدوث أخطاء عند استخدام الطريقة اليدوية يكون أكبر منه عند استخدام بروتوكول DHCP . تتم عملية عنونة DHCP Clients بعنوان الـ IP باستخدام بروتوكول DHCP.

إنّ بروتوكول DHCP وكالكثير من بروتوكولات أو خدمات الشبكة يقوم مبدأ عمله على خادم «Server» وعميل «Client» ، ولكن يجب التطرق إلى مصطلح هام وهو «Lease» والتي تعبّر عن الفترة الزمنية التي يقوم من خلالها الـ DHCP Client باستخدام عنوان الـ IP والإعدادات الأخرى التي حصل عليها من الـ DHCP Server .

وتسمى عملية إعطاء عنوان IP والإعدادات الأخرى من DHCP Server إلى DHCP Client باسم Lease Generation Process, حيث أنّ هذه العملية تتم من خلال تبادل بعض الرسائل على شكل Broadcast Messages بين DHCP Client و DHCP Server ، والتي قد تكون أشبه بالعطاء التجاري إلى حد ما, وهذه الرسائل أو الخطوات هي :

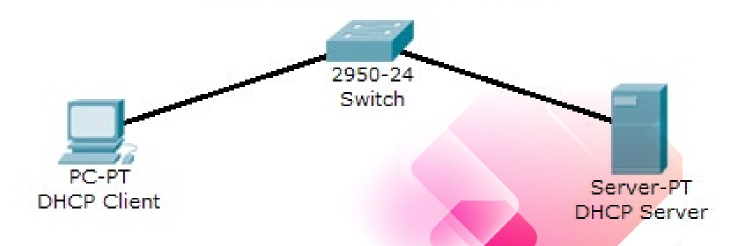
1. في الخطوة الأولى من العطاء التجاري يقوم طالب العطاء بنشر إعلانات عن هذا العطاء في الصحف والوسائل الإعلامية الأخرى ليبحث فيها عن الراغبين في المشاركة في هذا العطاء ، وفي بروتوكول DHCP يقوم DHCP Client بإرسال Broadcast DHCPDISCOVER Message والتي تُستخدم للبحث من خلالها عن DHCP Server في الشبكة المحلية .

2. في الخطوة الثانية يقوم التُجّار أو الراغبين بالمشاركة في العطاء بإرسال عروضهم إلى الجهة المعنيّة ، أما بالنسبة لبروتوكول DHCP يقوم DHCP Server's الموجود في الشبكة والذي قام باستلام الرسالة السابقة بالرد عليه بإرسال Broadcast DHCPOFFER Message, والذي يعرض فيها عنوان IP وإعدادات أخرى على DHCP Client .
حيث أنّ كل DHCP Server يقوم بإرسال OFFER لـ DHCP Client, كما أنّ عنوان الـ IP الذي يتم عرضه على Client معيّن, لن يتم عرضه لـ Client آخر إلّا بعد أن يرسل الـ Client الأول REQUEST . ففي حال أنّ DHCP Client لم يستلم أيّ رسائل OFFER بعد أربعة محاولات من إرسال DISCOVER Messages فإنّه يستخدم تقنية APIPA لعمل إعداداته .

3. يقوم ناشر العطاء باختيار إحدى هذه العروض ليرسو عليها العطاء ، وكذلك يقوم DHCP Client بإرسال DHCPREQUEST Broadcast

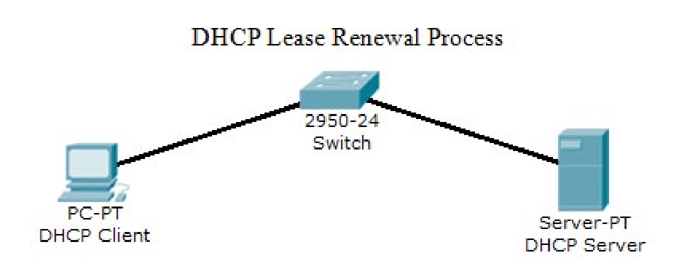
Message إلى DHCP Server معيّن ليطلب منه Lease لعنوان IP ، حيث يقوم DHCP Client بالاستجابة لأول DHCPOFFER Message استقبلها ، حيث أنّ الـ DHCPREQUEST يحتوي على مُعرّف خاص بالـ Server الذي تم قبول عرضه ، وعندها يقوم كل DHCP Server آخر قام بإرسال عرض باستعادة ذلك العرض والاحتفاظ به لأي عملية Lease Generation أخرى .

4. وبعدها يتم توريد الأجهزة أو أياً كان من المواد المتفق عليها بالعطاء من الشركة التي ربحت العطاء إلى طالب العروض ، وهذا ما يقوم به DHCP Server الذي تم قبول عرضه بإرسال Broadcast DHCPACK Message إلى DHCP Client ليؤكّد له أنّ إعدادات Lease التي طلبها قد اكتملت وتحتوي هذه الـ Packet على عنوان الـ IP والإعدادات الأخرى .



هذه كانت خطوات حصول DHCP Client على عنوان الـ IP والإعدادات الأخرى من DHCP Server, ولكن كما ذكرت سابقاً فإنّ الـ Lease تُحدد فترة زمنية معينة للاحتفاظ بهذه الإعدادات ، وبالتالي فإنّه لا بد من وجود طريقة لتجديد هذه الـ Lease, حيث تسمى هذه العملية بـ DHCP Lease Renewal Process ، والتي تهدف إلى تنظيم عمل بروتوكول DHCP من حيث متابعة العناوين التي لا تزال مستخدمة والتي انتهى استخدامها, كما أنّ هذه العملية تضمن تحديث وتجديد لعنوان الـ IP والإعدادات الأخرى بشكل منتظم .

إنّ عملية تجديد الـ Lease يمكن أن تتم إما بشكل يدوي أو بشكل أوتوماتيكي ، حيث أنّ الطريقة اليدوية تتم بالوقت الذي يريده الـ Client وباستخدام أوامر بسيطة على جهاز DHCP Client ، أما بالنسبة للطريقة الأوتوماتيكية تتلخص في محاولة DHCP Client لتجديد الـ Lease والتي يجب أن تتم قبل انتهاء مدة الـ Lease , حيث أنّه بعد انقضاء 50٪ من مدة الـ Lease يقوم DHCP Client بمحاولة تجديد الـ Lease وذلك بإرسال Unicast DHCPREQUEST Message لـ DHCP Server الذي حصل منه على الـ Lease ، فإذا كان DHCP Server متوفراً في الشبكة فإنّه يجدد الـ Lease ويرسل Unicast DHCPACK Message إلى الـ Client ، أما إذا لم يكن DHCP Server متوفراً في الشبكة فإنّ الـ Client يستمر باستخدام الـ Lease المتوفرة لديه .



فإذا فشلت محاولة تجديد الـ Lease بعد مرور 50٪ من عمرها الزمني, فإنّ DHCP Client يقوم بإرسال Broadcast DHCPDISCOVER Message بعد مرور 87.5٪ من مدة الـ Lease, ويقبل حينها أي رد من أي DHCP Server في الشبكة .


NetWork Set
First Arabic Magazine For Networks
www.networkset.net